IT Governance Using CobiT® and Val IT™:

Student Book, 2nd Edition

Taking professional practices to higher education

IT Governance Institute®

Leading the IT Governance Community

IT Governance Institute®
The IT Governance Institute (ITGI™) (*www.itgi.org*) was established in 1998 to advance international thinking and standards in directing and controlling an enterprise's information technology. Effective IT governance helps ensure that IT supports business goals, optimises business investment in IT, and appropriately manages IT-related risks and opportunities. ITGI offers original research and case studies to assist enterprise leaders and boards of directors in their IT governance responsibilities.

Disclaimer
ITGI and the author of *IT Governance Using COBIT® and Val IT™: Student Book, 2nd Edition* have designed the publication primarily as an educational resource for educators. ITGI, ISACA® and the authors make no claim that use of this product will assure a successful outcome. The publication should not be considered inclusive of all proper procedures and tests or exclusive of all proper procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific procedure or test, controls professionals should apply their own professional judgement to the specific control circumstances presented by the particular systems or IT environment. Note that this publication is an update of *COBIT® in Academia: Student Book*.

IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.590.7491
Fax: +1.847.253.1443
E-mail: *info@itgi.org*
Web site: *www.itgi.org*

ISBN 978-1-60420-024-9
IT Governance Using COBIT® and Val IT™: Student Book, 2nd Edition
Printed in the United States of America

ACKNOWLEDGEMENTS

ITGI wishes to recognise:

Researcher
Ed O'Donnell, University of Kansas, USA

Contributors
Roger Stephen Debreceny, Ph.D., FCPA, University of Hawaii, USA
Steven DeHaes, University of Antwerp Management School, Belgium
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium
Robert Parker, CISA, CA, CMC, FCA, Canada
V. Sambamurthy, Ph.D., Michigan State University, USA
Scott Lee Summers, Ph.D., Brigham Young University, USA
John Thorp, The Thorp Network, Canada
Wim Van Grembergen, Ph.D., University of Antwerp (UA) and University of Antwerp Management School (UAMS) and IT Alignment and Governance Research Institute (ITAG), Belgium
Ramesh Venkataraman, Ph.D., Indiana University, USA

ITGI Board of Trustees
Everett C. Johnson, CPA, Deloitte & Touche (retired), USA, International President
Georges Ataya, CISA, CISM, CISSP, ICT Control sa-nv, Belgium, Vice President
William C. Boni, CISM, Motorola, USA, Vice President
Lucio Augusto Molina Focazzio, CISA, Colombia, Vice President
Avinash Kadam, CISA, CISM, CBCP, CISSP, Miel e-Security Pvt. Ltd., India, Vice President
Jean-Louis Leignel, MAGE Conseil, France, Vice President
Howard Nicholson, CISA, City of Salisbury, Australia, Vice President
Frank Yam, CISA, CIA, CCP, CFE, CFSA, FFA, FHKCS, FH KIoD, Focus Strategic Group, Hong Kong, Vice President
Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, Past International President
Robert S. Roussey, CPA, University of Southern California, USA, Past International President
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada, Trustee

IT Governance Committee
Tony Hayes, FCPA, Queensland Government, Australia, Chair
Max Blecher, Virtual Alliance, South Africa
Sushil Chatterji, Singapore
Anil Jogani, CISA, FCA, Tally Solutions Limited, UK
John W. Lainhart, IV, CISA, CISM, CIPP/G, IBM, USA
Romulo Lomparte, CISA, Banco de Credito BCP, Peru
Michael Schirmbrand, Ph.D., CISA, CISM, CPA, KPMG LLP, Austria
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada

ITGI Advisory Panel
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada, Chair
Roland Bader, F. Hoffmann-La Roche AG, Switzerland
Linda Betz, IBM Corporation, USA
Jean-Pierre Corniou, Renault, France
Rob Clyde, CISM, Symantec, USA
Richard Granger, NHS Connecting for Health, UK
Howard Schmidt, CISM, R&H Security Consulting LLC, USA
Alex Siow Yuen Khong, StarHub Ltd., Singapore
Amit Yoran, Yoran Associates, USA

ACKNOWLEDGEMENTS (*CONT.*)

Academic Relations Committee
Scott Lee Summers, Ph.D., Brigham Young University, USA, Chair
Casey G. Cegielski, Ph.D., CISA, Auburn University, USA
Patrick Hanrion, CISM, CISSP, CNE, MCSE, Microsoft, USA
Donna Hutcheson, CISA, XR Group Inc., USA
Cejka Jiri Josef, CISA, Dipl. El. -Ing., KPMG Fides Peat, Switzerland
Michael Lambert, CISA, CISM, CARRA, Canada
Ed O'Donnell, University of Kansas, USA
Theodore Tryfonas, Ph.D., CISA, University of Glamorgan, Wales
Ramesh Venkataraman, Ph.D., Indiana University, USA

COBIT Steering Committee
Roger Stephen Debreceny, Ph.D., FCPA, University of Hawaii, USA, Chair
Gary S. Baker, CA, Deloitte & Touche, Canada
Steven DeHaes, University of Antwerp Management School, Belgium
Rafael Eduardo Fabius, CISA, Republica AFAP, S.A., Uruguay
Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Switzerland
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium
Gary Hardy, IT Winners, South Africa
Jimmy Heschl, CISM, CISA, KPMG, Austria
Debbie A. Lew, CISA, Ernst & Young LLP, USA
Maxwell J. Shanahan, CISA, FCPA, Max Shanahan & Associates, Australia
Dirk E. Steuperaert, CISA, PricewaterhouseCoopers LLC, Belgium
Robert E. Stroud, CA Inc., USA

ITGI Affiliates and Sponsors
ISACA chapters
American Institute for Certified Public Accountants
ASIS International
The Center for Internet Security
Commonwealth Association of Corporate Governance Inc.
FIDA Inform
Information Security Forum
Information Systems Security Association
Institut de la Gouvernance des Systèmes d'Information
Institute of Management Accountants
ISACA
ITGI Japan
Solvay Business School
University of Antwerp Management School
Aldion Consulting Pte. Ltd.
CA
Hewlett-Packard
IBM
ITpreneurs Nederlands BV
LogLogic Inc.
Phoenix Business and Systems Process Inc.
Project Rx Inc.
Symantec Corporation
Wolcott Group LLC
World Pass IT Solutions

TABLE OF CONTENTS

1. PURPOSE OF THIS DOCUMENT

The goal of *IT Governance Using COBIT® and Val IT™: Student Book, 2nd Edition*, is to provide high-quality educational material that can be integrated into courses on information systems, management control or assurance services. This document provides overviews of:
- IT governance
- The *Control Objectives for Information and related Technology* (COBIT®) framework for IT controls
- IT assurance initiatives
- Audits of IT controls over financial reporting

The *Student Book, 2nd Edition*, was developed by ITGI, in collaboration with a group of international academics and practitioners, by assembling excerpts from other ITGI publications.

The objective in creating this document was to develop a learning resource that can be used effectively by students with little or no business experience. As a result, the ITGI materials reproduced herein have been abridged by removing material that addresses practical and operational issues that are of concern to business people and information technology (IT) professionals, but may be difficult for students to appreciate and comprehend.

Chapter 2, Governing IT Resources, describes IT governance practices and how an organisation can create business value through IT investments. Material for chapter 2 was assembled from the *Board Briefing on IT Governance, 2nd Edition* and *Enterprise Value: Governance of IT Investments—The Val IT Framework*. Students will learn how organisations manage IT resources to deliver stakeholder value through strategic alignment, value delivery, risk management and performance measurement. This chapter also describes how organisations can manage their IT investments as a portfolio.

Chapter 3, Managing IT Risks, presents a framework of control objectives designed to help an organisation manage risks that threaten information and related technology. Material for chapter 3 was assembled from *COBIT® 4.1*. Students will learn how to establish control objectives for planning and organising the IT function, acquiring and implementing IT capabilities, delivering and supporting IT functions, and monitoring and evaluating IT service delivery. This chapter also discusses the role of IT application controls in a risk management initiative.

Chapter 4, Providing IT Assurance, describes the processes that assurance professionals use to evaluate and report on the effectiveness of IT controls. Material for chapter 4 was assembled from the *IT Assurance Guide Using COBIT®*. Students will learn how to develop a plan for IT assurance initiatives, scope the initiative by identifying key control objectives, and test the design and operating effectiveness of control procedures designed to address key control objectives. This chapter also provides examples of how to test the design and operating effectiveness of IT controls, and evaluate the impact of control weaknesses.

Chapter 5, Auditing IT Controls Over Financial Reporting, outlines the process for auditing IT controls over financial reporting. Material for chapter 5 was assembled from *IT Control Objectives for Sarbanes-Oxley, 2nd Edition*. Students will learn about the process for auditing IT general controls over financial reporting, including how to plan and scope an evaluation, assess IT risk, document IT controls, evaluate the design and operating effectiveness of IT controls, and build sustainability into the evaluation process.

2. GOVERNING IT RESOURCES

Increasingly, top management is realising the significant impact that IT can have on the success of the enterprise. Management hopes for heightened understanding of the way IT is operated and the likelihood of its being leveraged successfully for competitive advantage. Boards and executive management need to extend governance to IT and provide the leadership, organisational structures and processes that ensure that the enterprise's IT sustains and extends the enterprise's strategies and objectives. IT governance is not an isolated discipline; it is an integral part of overall enterprise governance.

The need to integrate IT governance with overall governance is similar to the need for IT to be an integral part of the enterprise rather than something practiced in remote corners or ivory towers. An increasingly educated and assertive set of stakeholders is concerned about the sound management of its interests. This has led to the emergence of governance principles and standards for overall enterprise governance. Furthermore, regulations establish board responsibilities and require that the board of directors exercise due diligence in its roles. Investors have also realised the importance of governance; research shows they are willing to pay a premium of more than 20 percent on shares of enterprises that have shown to have good governance practices in place.[1]

Enterprise governance is a set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly. While governance developments have primarily been driven by the need for the transparency of enterprise risks and the protection of shareholder value, the pervasive use of technology has created a critical dependency on IT that calls for a specific focus on IT governance.

IT is essential to manage the transactions, information and knowledge necessary to initiate and sustain economic and social activities. In most enterprises, IT has become an integral part of the business and is fundamental to support, sustain and grow the business. Successful enterprises understand and manage the risks and constraints of IT. Increasingly, boards of directors understand the strategic importance of IT and have put IT governance firmly on their agenda.

WHAT IS IT GOVERNANCE?

The overall objective of IT governance is to understand the issues and strategic importance of IT so the enterprise can sustain its operations and implement the strategies required to extend its activities into the future. IT governance aims to ensure that expectations for IT are met and IT risks are mitigated. IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives.

At the heart of the governance responsibilities of setting strategy, managing risks, delivering value and measuring performance are the stakeholder values, which drive the enterprise and IT strategy. Sustaining the current business and growing into new business models certainly are stakeholder expectations, and can be achieved only with adequate governance of the enterprise's IT infrastructure.

The purpose of IT governance is to direct IT endeavors, to ensure that IT's performance meets the following objectives:
- Alignment of IT with the enterprise and realisation of the promised benefits
- Use of IT to enable the enterprise by exploiting opportunities and maximising benefits
- Responsible use of IT resources
- Appropriate management of IT-related risks

WHY IS IT GOVERNANCE IMPORTANT?

The use of IT has the potential to be the major driver of economic wealth in the 21st century. Whilst IT is already critical to enterprise success, provides opportunities to obtain a competitive advantage and offers a means for increasing productivity, it will do all this to an even greater extent in the future. Successfully leveraging IT to transform the enterprise and create value-added products and services has become a universal business competency. IT is fundamental for managing enterprise resources, dealing with suppliers and customers, and enabling increasingly global transactions.

[1] McKinsey's Investors Opinion Survey, June 2000

IT also is key for recording and disseminating business knowledge. An ever larger percentage of the market value of enterprises has transitioned from the tangible (inventory, facilities, etc.) to the intangible (information, knowledge, expertise, reputation, trust, patents, etc.). Many of these assets revolve around the use of IT. Moreover, a firm is inherently fragile if its value emanates more from conceptual, rather than physical, assets.

Therefore, good governance of IT is critical in supporting and enabling enterprise goals. Whilst IT is fundamental to sustain what may be unglamorous and taken-for-granted business operations, it is equally essential for business growth and innovation. Those with a strict commercial focus may challenge the latter but should be aware that unwillingness to innovate limits the prospects of achieving future goals and long-term sustainability.

IT also carries risks. It is clear that, in these days of doing business on a global scale and around the clock, system and network downtime has become far too costly for any enterprise. In some industries, IT is a necessary competitive resource to differentiate and provide a competitive advantage, whilst in many others it determines not just prosperity but survival. The networked economy has brought more efficient markets, enabled streamlining of processes and optimised supply chains. It has also created new technology and business risks and new information and resilience requirements. These new requirements and risks mandate that management of IT be more effective and transparent.

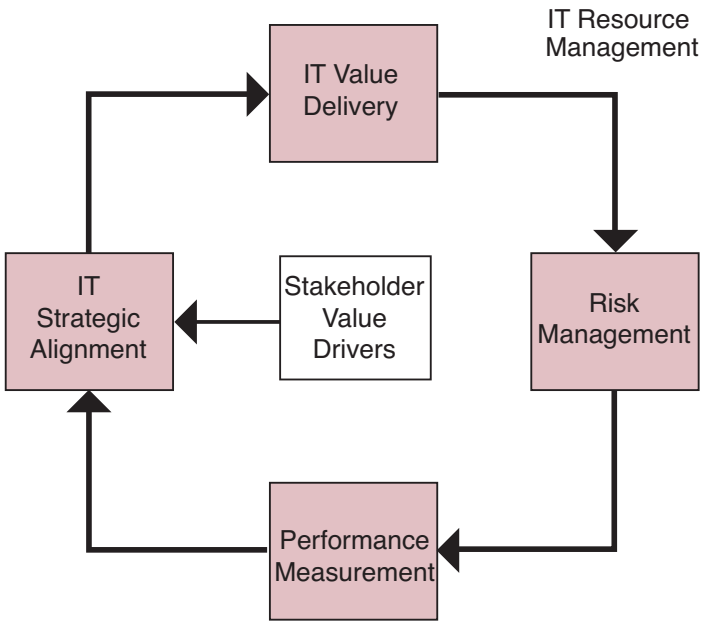
WHAT DOES IT GOVERNANCE COVER?

Fundamentally, IT governance is concerned about two things: IT's delivery of value to the business and the mitigation of IT risks. The first is driven by strategic alignment of IT with the business. The second is driven by embedding accountability into the enterprise. Both need to be supported by adequate resources and measured to ensure that the results are obtained.

IT governance is also a process through which the IT strategy drives the IT processes, which obtain resources necessary to execute their responsibilities. The IT processes report against these responsibilities on process outcome, performance, risks mitigated and accepted, and resources consumed. These reports should either confirm that the strategy is properly executed or provide indications that strategic redirection is required.

This leads to the five main focus areas for IT governance, all driven by stakeholder value. Two of them are outcomes: value delivery and risk management. Three of them are drivers: strategic alignment, resource management (which overlays them all) and performance measurement. These associations are illustrated in **figure 1**.

Figure 1—Focus Areas of IT Governance



IT governance is also a continuous life cycle that can be entered at any point. Usually one starts with the strategy and its alignment throughout the enterprise. Then implementation occurs, delivering the value the strategy promised and addressing the risks that need mitigation. At regular intervals (some recommend continuously), the strategy needs to be monitored and the results measured, reported and acted upon. Generally on an annual basis, the strategy is re-evaluated and realigned, if needed. This life cycle does not take place in a vacuum. Each enterprise operates in an environment that is influenced by:

- Stakeholder values
- The mission, vision and values of the enterprise
- The community and company ethics and culture
- Applicable laws, regulations and policies
- Industry practices

Strategic Alignment

To be aligned, an enterprise's investment in IT must be in harmony with its strategic objectives (intent, current strategy and enterprise goals) to build the capabilities necessary to deliver business value. This state of harmony is referred to as 'alignment'. It is complex, multifaceted and never completely achieved. It is about continuing to move in the right direction and being better aligned than competitors. This may not be attainable for many enterprises because enterprise goals change too quickly, but it is nevertheless a worthwhile ambition because there is real concern about the value of IT investment.

Alignment of IT has been synonymous with IT strategy, i.e., does the IT strategy support the enterprise strategy? For IT governance, alignment encompasses more than strategic integration between the (future) IT organisation and the (future) enterprise organisation. It also is about whether IT operations are aligned with the current enterprise operations. The IT strategy articulates the enterprise's intention to use IT for some or all of these reasons, based on business requirements. Linkage to the business aims is essential for IT to deliver recognisable value to the enterprise.

When formulating the IT strategy, management must consider business objectives; the competitive environment; and current and future technologies, including the costs, risks and benefits they can bring to the business. Management must also consider the capability of the IT organisation to deliver current and future levels of service to the business, and the extent of change and investment this might imply for the whole enterprise.

It is important that the plan for implementing the strategy be endorsed by all relevant parties. It is also important that the implementation plans be broken down into manageable parts, each with a clear business case incorporating a plan for achieving outcomes and realising benefits. The board should ensure that the strategy is reviewed regularly in light of technological and operational change.

Value Delivery

The basic principles of IT value are the on-time and within-budget delivery of appropriate quality, which achieves the benefits that were promised. In business terms, this is often translated into competitive advantage, elapsed time for order/service fulfillment, customer satisfaction, customer wait time, employee productivity and profitability. Several of these elements are either subjective or difficult to measure, something all stakeholders need to understand. Often, top management and boards fear to start major IT investments because of the size of investment and the uncertainty of the outcome. For effective IT value delivery to be achieved, both the actual costs and the return on investment (ROI) need to be managed.

The value that IT adds to the business is a function of the degree to which the IT organisation is aligned with the business and meets the expectations of the business. The business should set expectations relative to the contents of the IT deliverable. To manage these expectations, IT and the business should use a common language for value, which translates business and IT terminology and is based wholly on fact.

Different levels of management and users perceive the value of IT differently—the higher one goes in the measurement hierarchy, the more dilution occurs (i.e., the less influence IT management can exercise). This also means that measuring the impact of an IT investment is much easier at the bottom of the hierarchy than at the top. However, successful investments in IT have a positive impact on all four levels of the business value hierarchy.

IT needs to be aligned to deliver value so that it supports the enterprise as it is by delivering on time, with appropriate functionality and achievement of the intended benefits. Alignment of IT also provides value by delivering infrastructures that enable the enterprise to grow by breaking into new markets, increasing overall revenue, improving customer satisfaction, assuring customer retention and driving competitive strategies.

To be successful, enterprises need to be aware that different strategic contexts require different indicators of value. This means that it is important to establish the value measures in concert between the business and IT. It should also be mentioned that the public sector has different value drivers/indicators than the private sector. In the public sector, measures such as compliance and due diligence take prominence over financial measures, such as profitability.

Risk Management

Enterprise risk comes in many varieties in addition to financial risk. Regulators are specifically concerned about operational and systemic risk, within which technology risk and information security issues are prominent. Infrastructure protection initiatives point to the complete dependence of all enterprises on IT infrastructures and the vulnerability to new technology risks.

The board should manage enterprise risk by:
- Ascertaining that there is transparency about the significant risks to the enterprise and clarifying the risk-taking or risk-avoidance policies of the enterprise (i.e., determining the enterprise's appetite for risk)
- Being aware that the final responsibility for risk management rests with the board, so, when delegating to executive management, making sure the constraints of that delegation are communicated and clearly understood
- Being conscious that the system of internal control put in place to manage risks often has the capacity to generate cost-efficiency
- Considering that a transparent and proactive risk management approach can create competitive advantage that can be exploited
- Insisting that risk management be embedded in the operation of the enterprise, respond quickly to changing risks and report immediately to appropriate levels of management, supported by agreed-upon principles of escalation (what to report, when, where and how)

Effective risk management begins with a clear understanding of the enterprise's appetite for risk and a brainstorming session on the high-level risk exposures of the enterprise. This focuses all risk management effort and, in an IT context, impacts future investments in technology, the extent to which IT assets are protected and the level of assurance required. At minimum, risk should at least be analysed, because even if no immediate action is taken, the awareness of risk will influence strategic decisions for the better. Often, the most damaging IT risks are those that are not well understood.

Performance Measurement

Strategy has taken on a new urgency as enterprises mobilise intangible and hidden assets to compete in an information-based global economy. The means of value creation has shifted from tangible to intangible assets, and intangible assets generally are not measurable through traditional financial means. Balanced scorecards translate strategy into action to achieve goals with a performance measurement system that goes beyond conventional accounting, measuring those relationships and knowledge-based assets necessary to compete in the information age (customer focus, process efficiency, and the ability to learn and grow).

Each perspective is designed to answer one question about the enterprise's way of doing business:
- Financial perspective—To satisfy our stakeholders, what financial objectives must we accomplish?
- Customer perspective—To achieve our financial objectives, what customer needs must we serve?
- Internal process perspective—To satisfy our customers and stakeholders, in which internal business processes must we excel?
- Learning perspective—To achieve our goals, how must our organisation learn and innovate?

By using the balanced scorecard, managers rely on more than short-term financial measures as indicators of the company's performance. They also take into account such intangible items as level of customer satisfaction, streamlining of internal functions, creation of operational efficiencies and development of staff skills. This unique and more holistic view of business operations contributes to linking long-term strategic objectives with short-term actions.

At the heart of these scorecards is management information supplied by relevant stakeholders and supported by a sustainable reporting system. But IT does more than provide information to obtain a global picture as to where the enterprise is and where it is going. IT also enables and sustains solutions for the actual goals set in the financial (enterprise resource management), customer (customer relationship management), process (intranet and workflow tools) and learning (knowledge management) dimensions of the scorecard.

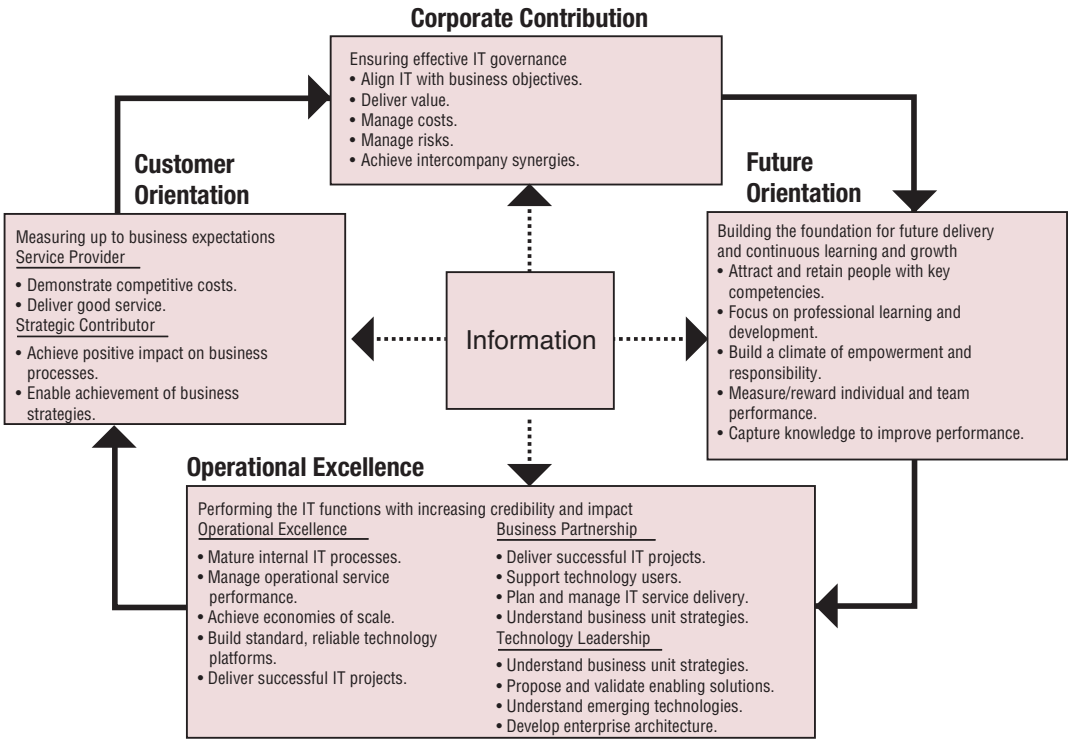
IT not only contributes information to the business scorecards and tools to the different dimensions being measured, but also—because of the criticality of IT itself—needs its own scorecard. Defining clear goals and good measures that unequivocally reflect the business impact of the IT goals is a challenge and needs to be resolved in co-operation amongst the different governance layers within the enterprise.

Use of an IT balanced scorecard (IT BSC) is one of the most effective means to aid the board and management to achieve IT and business alignment. The objectives are to establish a vehicle for management reporting to the board; foster consensus amongst key stakeholders about IT's strategic aims; demonstrate the effectiveness and added value of IT; and communicate about IT's performance, risks and capabilities.

To apply the balanced scorecard concepts to the IT function, the four perspectives need to be redefined. An IT BSC template can be developed by considering the following questions:
- Corporate contribution—How do business executives view the IT department?
- Customer orientation—How do users view the IT department?
- Operational excellence—How effective and efficient are the IT processes?
- Future orientation—How well is IT positioned to meet future needs?

Demonstrating the value IT delivers to the business requires cause-and-effect relationships between two types of measures throughout the scorecard outcomes measures (measuring what you have done) and performance drivers (measuring how you are doing). **Figure 2** summarises the objectives of each specific area from which measures can be derived.

Figure 2—Sample IT BSC Measures



Managing IT Resources

Enterprises should align and prioritise the existing IT services that are required to support business operations based on clear service definitions. These definitions and related performance metrics enable business-oriented service level agreements (SLAs) providing a basis for effective oversight and monitoring of both internal and outsourced IT services. The IT assets should be organised so that the required quality of service is provided by the most cost-effective delivery infrastructure. Companies that achieve this not only realise great cost savings, but also are well placed to take on the next new IT initiative, judiciously introducing new technologies and replacing or updating obsolete systems.

A key to successful IT performance is the optimal investment, use and allocation of IT resources (people, applications, technology, facilities, data) in servicing the needs of the enterprise. In most enterprises, the biggest portion of the IT budget relates to ongoing operations. Of all the IT assets, human resources represent the biggest part of the cost base and, on a unit basis, the one most likely to increase. It is essential to identify and anticipate the required core competencies in the workforce. When these are understood, an effective recruitment, retention and training programme is necessary to ensure that the organisation has the skills to utilise IT effectively to achieve the stated objectives.

Effective governance of IT operational spending requires effective control of the cost base. IT assets are complex to manage and continually change due to the nature of technology and changing business requirements. Effective management of the life cycle of hardware, software licences, service contracts, and permanent and contracted human resources is a critical success factor not only for optimising the IT cost base, but also for managing changes, minimising service incidents and assuring a reliable quality of service.

Many organisations have created value through selection of the right investments and effective management of the investments from concept through implementation to realisation of the expected value. Examples include IBM, which reportedly was able to save more than US $12 billion over two years by linking disparate pieces of its supply chain, thereby reducing inventory levels, and Southwest Airlines, which was able to reduce procurement costs and increase service levels through its supply chain transformation project.

The message is clear. IT-enabled business investments can bring huge benefits. Indeed, a study carried out within global financial services group ING indicates that IT-enabled business investments offer the opportunity to deliver greater returns than almost any other conventional investment. This research, carried out in mid-2004, indicated that, in comparison to more traditional investments such as commercial real estate, publicly traded equities and sovereign bonds, the return on a well-balanced portfolio of IT-enabled business investments can be expected to be significantly higher. However, the result of getting it wrong can be significant, including catastrophic financial losses and competitive disadvantage.

The level of investment in IT is significant and continues to increase. Few organisations could operate for long today without their IT infrastructure. Yet, while there are many examples of organisations generating value from investing in IT, at the same time, many executives are questioning whether the business value realised is commensurate with the level of investment. IT-enabled business investments, when managed well within an effective governance framework, provide organisations with significant opportunities to create value. Without effective governance and good management, they provide an equally significant opportunity to destroy value.

Creating Value Through IT Investments

Value is not a simple concept. It is complex, context-specific and dynamic. Value is, indeed, 'in the eye of the beholder'. The nature of value differs for different types of organisations. For commercial or for-profit organisations, value tends to be viewed primarily in financial terms and can be simply the increase in profit to the organisation that arises from the investment. For not-for-profit organisations, including the public sector, value is more complex and is often non-financial in nature. It should be the improvement in the organisation's performance against business metrics (which measure what is provided to those whom the organisation exists to serve) and/or the net increase in income that is available to provide those services, either or both of which arise from the investment.

Business value is generated by what organisations do with IT rather than by the technology itself. There is a clear incentive for management to ensure that the right governance and management processes are in place to optimise the creation of value. Ensuring that value is obtained from IT-enabled investments is an essential component of enterprise governance. It involves selecting investments wisely and managing them as an asset or service throughout their life cycle.

Value delivery is one of the five focus areas of IT governance, alongside strategic alignment, performance measurement, resource management and risk management. Indeed, unless success is achieved in the other four focus areas, achieving value delivery will remain elusive. Recent studies state, 'Effective IT governance is the single most important predictor of the value an organisation generates from IT' and 'firms with focused strategies and above average IT governance had more than 20 percent higher profits than other firms following the same strategies'.[2]

Effective governance starts with leadership, commitment and support from the top. However, such leadership, whilst critical, is not enough. Leadership initiatives must be supported by consistently applied processes; a clear understanding of executive, business and IT roles and responsibilities; relevant information; and appropriate organisational structures. The enterprise needs to establish processes, practices and metrics to support consistent and transparent decision making.

[2] Center for Information Systems Research (CISR)

IT-enabled business investments should be treated like any other investment decision, where the investor balances opportunity, return and risk whilst looking for assurance that the benefits will be delivered. The key challenge is to ensure that the expected and risk-adjusted benefits respond to the goals set for the investment. An organisation must implement and sustain three processes that are essential for creating value from IT investments, including value governance, portfolio management and investment management.

The goal of value governance is to optimise the value of an organisation's IT-enabled investments by establishing the governance, monitoring and control framework. The control framework defines the processes and activities (relative to the governance of IT-enabled business investments) that occur within the context of overall enterprise governance. Value governance also includes providing strategic direction for the investments and defining the investment portfolio characteristics.

The goal of portfolio management is to ensure that an organisation's overall portfolio of IT-enabled investments is aligned with, and contributing optimal value to, the organisation's strategic objectives. IT-enabled business investment programmes are managed as a portfolio of investments. The programmes in the portfolio must be clearly defined, evaluated, prioritised, selected and managed actively throughout their full economic life cycle to optimise value for individual programmes and the overall portfolio. This includes the proper allocation of resources, the management of risk, the early identification and correction of problems (including programme cancellation, if appropriate), and board-level programme portfolio oversight.

Portfolio management recognises the requirement for a balanced portfolio. It also recognises that there are different categories of investment with differing levels of complexity and degrees of freedom in allocating funds. Evaluation criteria with appropriate weightings are established for each category of investment. The decision to include a programme in the portfolio is not a one-time decision. The portfolio is actively managed and, depending on the relative performance of programmes within the portfolio and changes to the internal or external business environment, the makeup of the portfolio may be adjusted.

The goal of investment management is to ensure that an organisation's individual IT-enabled investment programmes deliver optimal value at an affordable cost with a known and acceptable level of risk. There are three key components of investment management:
- Business case development—Supporting selection of the right investment programmes
- Programme management—Managing execution of the programmes
- Benefits realisation—Actively managing the realisation of benefits from the programmes

The seeds of success or failure are sown in the business case. The business case contains a set of beliefs and assumptions on how value can be created. To ensure that the expected outcomes will be achieved, these beliefs and assumptions need to be well tested. Qualitative and quantitative indicators enable validation of the business case and provide insight for future investment decisions. This is where it all starts. The ITGI publication, *Enterprise Value: Governance of IT Investments—The Business Case*, provides guidance to maximise the quality of business cases, with particular emphasis on the definition of key indicators, both financial (net present value, internal rate of return and payback period) and non-financial, and the comprehensive assessment and appraisal of the downside risk.

The basic content of the business case consists of the major input resources and three activity streams leading to delivering technical capabilities, operational capabilities and business capabilities resulting in financial return or other non-financial outcomes. Each of these streams needs to be documented with data to support the investment decision and portfolio management processes initiatives, costs, risks, assumptions and outcomes.

The business case should be developed top-down, starting with a clear understanding of the desired business outcomes. Once an investment is approved, the delivery of the required capabilities and the desired outcomes must be diligently monitored and controlled through the full economic life cycle of the investment. The business case is not a one-time, static document. It is an operational tool that must be continually updated to reflect the current reality and to support the portfolio management process.

IT alone does not deliver business value. It is only when IT is implemented in conjunction with associated changes in the business, business processes, individuals' work and competencies, and necessary organisational changes that value is realised. All of the changes that are required must be understood, defined and managed as a programme of IT-enabled change.

There must be clarity of the desired business outcomes, the full scope of initiatives required to achieve the outcomes, the relationship between the initiatives and how they individually and collectively contribute to the outcomes, and any assumptions that are being made related to those contributions or to the outcomes themselves. This requires the IT function and the other parts of the business to work closely together with clearly understood roles and responsibilities and shared accountabilities.

Benefits do not just happen, and they rarely happen according to plan. Benefits do not automatically start flowing with the implementation. If value is to be created, it is essential that investment programmes and the benefits expected from the programmes be actively managed through their full economic life cycle—from concept to cash. Organisations traditionally are very bad at this, but if it is not done, effective governance cannot be achieved, value will be eroded, and the business will not learn and improve its business case and portfolio management processes.

CONCLUSION

It is the responsibility of the board and top-level management to ensure that shareholder and stakeholder returns are optimised through judicious use of the resources and opportunities available. This responsibility includes IT-enabled business investments and resources where costs, the visibility of success or failure, and the risks of value destruction are high, but the potential for significant value creation is apparent.

IT governance fits in the broader governance arrangements that cover relationships between the entity's management and its governing body, its owners and its other stakeholders. It provides the structure through which the entity's IT objectives are set, the method of attaining those objectives is outlined and the manner in which performance will be monitored is described.

An IT governance framework helps boards and management understand the issues and strategic importance of IT, and assists in ensuring that the enterprise can sustain its operations and implement the strategies required to extend its activities into the future. Effective IT governance ensures that IT goals are met and IT risks are mitigated such that IT delivers value to sustain and grow the enterprise. IT governance drives strategic alignment between IT and the business, and must judiciously measure performance.

3. MANAGING IT RISKS

For many enterprises, information and the technology that supports it represent their most valuable, but often least understood, assets. Successful enterprises recognise the benefits of information technology and use it to drive their stakeholders' value. These enterprises also understand and manage the associated risks, such as increasing regulatory compliance and critical dependence of many business processes on IT. Managing risks requires a framework for control over IT that fits with and supports the Committee of Sponsoring Organisations of the Treadway Commission (COSO) *Internal Control—Integrated Framework*, the widely accepted control framework for enterprise governance and risk management, and similar compliant frameworks.

COBIT provides good practices across a domain and process framework, and presents activities in a manageable and logical structure. COBIT's good practices represent the consensus of experts. They are strongly focused on control and less so on execution. These practices will help optimise IT-enabled investments, ensure service delivery and provide a measure against which to judge when things do go wrong.

The business orientation of COBIT consists of linking business goals to IT goals, providing metrics and maturity models to measure their achievement, and identifying the associated responsibilities of business and IT process owners. The process focus of COBIT is illustrated by a process model that subdivides IT into 34 processes in line with the responsibility areas of plan, build, run and monitor, providing an end-to-end view of IT. Operational management uses processes to organise and manage ongoing IT activities. COBIT provides a generic process model that represents all the processes normally found in IT functions, providing a common reference model understandable to operational IT and business managers.

To achieve effective governance, executives expect controls to be implemented by operational managers within a defined control framework for all IT processes. COBIT's IT control objectives are organised by IT process; therefore, the framework provides a clear link amongst IT governance requirements, IT processes and IT controls. The COBIT process model has been mapped to IT governance focus areas, providing a bridge between what operational managers need to execute and what executives wish to govern.

In summary, COBIT is a framework and supporting tool set that allow managers to bridge the gap with respect to control requirements, technical issues and business risks, and communicate that level of control to stakeholders. COBIT enables the development of clear policy and good practice for IT control throughout enterprises. COBIT is continuously kept up to date and harmonised with other standards. Hence, COBIT has become the integrator for IT best practices and the umbrella framework for IT governance that helps in understanding and managing the risks and benefits associated with IT. The process structure of COBIT and its high-level business-oriented approach provide an end-to-end view of IT and the decisions to be made about IT.

THE COBIT FRAMEWORK

Governance and control frameworks are becoming a part of IT management best practice and are an enabler for establishing IT governance and complying with continually increasing regulatory requirements. IT best practices have become significant due to a number of factors:

- Business managers and boards demanding a better return from IT investments and concern over the generally increasing amount of IT expenditures
- The need to meet regulatory requirements for IT controls in areas such as financial reporting and in specific sectors such as finance, pharmaceutical and healthcare
- The selection of service providers and the management of service outsourcing and acquisition
- Increasingly complex IT-related risks, such as network security
- IT governance initiatives that include adoption of control frameworks and best practices to help monitor and improve critical IT activities to increase business value and reduce business risk
- The need for enterprises to assess how they are performing against generally accepted standards and against their peers (benchmarking)

Business orientation is the main theme of COBIT. It is designed to be employed not only by IT service providers, users and auditors, but also as comprehensive guidance for management and business process owners. Defining a set of generic business and IT goals provides a more refined basis for establishing business requirements and developing the metrics that allow measurement against these goals. Every enterprise uses IT to enable business initiatives, and these can be represented as business goals for IT. Once the goals have been defined, they need to be monitored to ensure that actual delivery matches expectations. This is achieved by metrics derived from the goals and captured in an IT scorecard that the customer can understand and follow, and that enables the provider to focus on its own internal objectives.

The IT organisation delivers against these goals by a clearly defined set of processes that use people skills and technology infrastructure to run automated business applications whilst leveraging business information. These resources, together with the processes, constitute an enterprise architecture for IT. To respond to the business requirements for IT, the enterprise needs to invest in the resources required to create an adequate technical capability [e.g., an enterprise resource planning (ERP) system] to support a business capability (e.g., implementing a supply chain) resulting in the desired outcome (e.g., increased sales and financial benefits). The IT resources identified in COBIT can be defined as follows:

- Applications are the automated user systems and manual procedures that process the information.
- Information is the data in all their forms input, processed and output by the information systems, in whatever form is used by the business.
- Infrastructure is the technology and facilities (hardware, operating systems, database management systems, networking, multimedia, etc., and the environment that houses and supports them) that enable the processing of the applications.
- People are the personnel required to plan, organise, acquire, implement, deliver, support, monitor and evaluate the information systems and services. They may be internal, outsourced or contracted as required.

COBIT defines IT activities in a generic process model within four domains. A process model encourages process ownership, enabling responsibilities and accountability to be defined. To govern IT effectively, it is important to appreciate the activities and risks within IT that need to be managed. These can be summarised as follows.

Plan and Organise (PO)

This domain covers strategy and tactics, and concerns the identification of the way IT can best contribute to the achievement of the business objectives. The realisation of the strategic vision needs to be planned, communicated and managed for different perspectives. A proper organisation as well as technological infrastructure should be put in place. This domain typically addresses the following management questions:

- Are IT and the business strategy aligned?
- Is the enterprise achieving optimum use of its resources?
- Does everyone in the organisation understand the IT objectives?
- Are IT risks understood and being managed?
- Is the quality of IT systems appropriate for business needs?

Acquire and Implement (AI)

To realise the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process. In addition, changes in and maintenance of existing systems are covered by this domain to make sure the solutions continue to meet business objectives. This domain typically addresses the following management questions:

- Are new projects likely to deliver solutions that meet business needs?
- Are new projects likely to be delivered on time and within budget?
- Will the new systems work properly when implemented?
- Will changes be made without upsetting current business operations?

Deliver and Support (DS)

This domain is concerned with the actual delivery of required services, which includes service delivery, management of security and continuity, service support for users, and management of data and the operational facilities. It typically addresses the following management questions:

- Are IT services being delivered in line with business priorities?
- Are IT costs optimised?
- Is the workforce able to use the IT systems productively and safely?
- Are adequate confidentiality, integrity and availability in place?

Monitor and Evaluate (ME)

All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain addresses performance management, monitoring of internal control, regulatory compliance and providing governance. It typically addresses the following management questions:

- Is IT's performance measured to detect problems before it is too late?

- Does management ensure that internal controls are effective and efficient?
- Can IT performance be linked back to business goals?
- Are risk, control, compliance and performance measured and reported?

In more detail, the overall COBIT framework can be shown graphically as in **figure 3**, with COBIT's process model of four domains containing 34 generic processes, managing the IT resources to deliver information to the business according to business and governance requirements. Descriptions of each control objective across the four domains are provided in appendix 1.

Controls-based

COBIT defines control objectives for all 34 processes, as well as overarching process and application controls. Control is defined as the policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented (or detected and corrected). IT control objectives provide a complete set of high-level requirements to be considered by management for effective control of each IT process. Control objectives are statements of managerial actions to increase value or reduce risk and are designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented (or detected and corrected).

The enterprise's system of internal controls impacts IT at three levels:

- At the executive management level, business objectives are set, policies are established, and decisions are made on how to deploy and manage the resources of the enterprise to execute the enterprise strategy. The overall approach to governance and control is established by the board and communicated throughout the enterprise. The IT control environment is directed by this top-level set of objectives and policies.
- At the business process level, controls are applied to specific business activities. Most business processes are automated and integrated with IT application systems, resulting in many of the controls at this level being automated as well. These controls are known as application controls. However, some controls within the business process remain as manual procedures, such as authorisation for transactions, separation of duties and manual reconciliations. Therefore, controls at the business process level are a combination of manual controls operated by the business and automated business and application controls. Both are the responsibility of the business to define and manage, although the application controls require the IT function to support their design and development.
- To support the business processes, IT provides IT services, usually in a shared service to many business processes, as many of the development and operational IT processes are provided to the whole enterprise, and much of the IT infrastructure is provided as a common service (e.g., networks, databases, operating systems and storage). The controls applied to all IT service activities are known as IT general controls. The reliable operation of these general controls is necessary for reliance to be placed on application controls. For example, poor change management could jeopardise (accidentally or deliberately) the reliability of automated integrity checks.

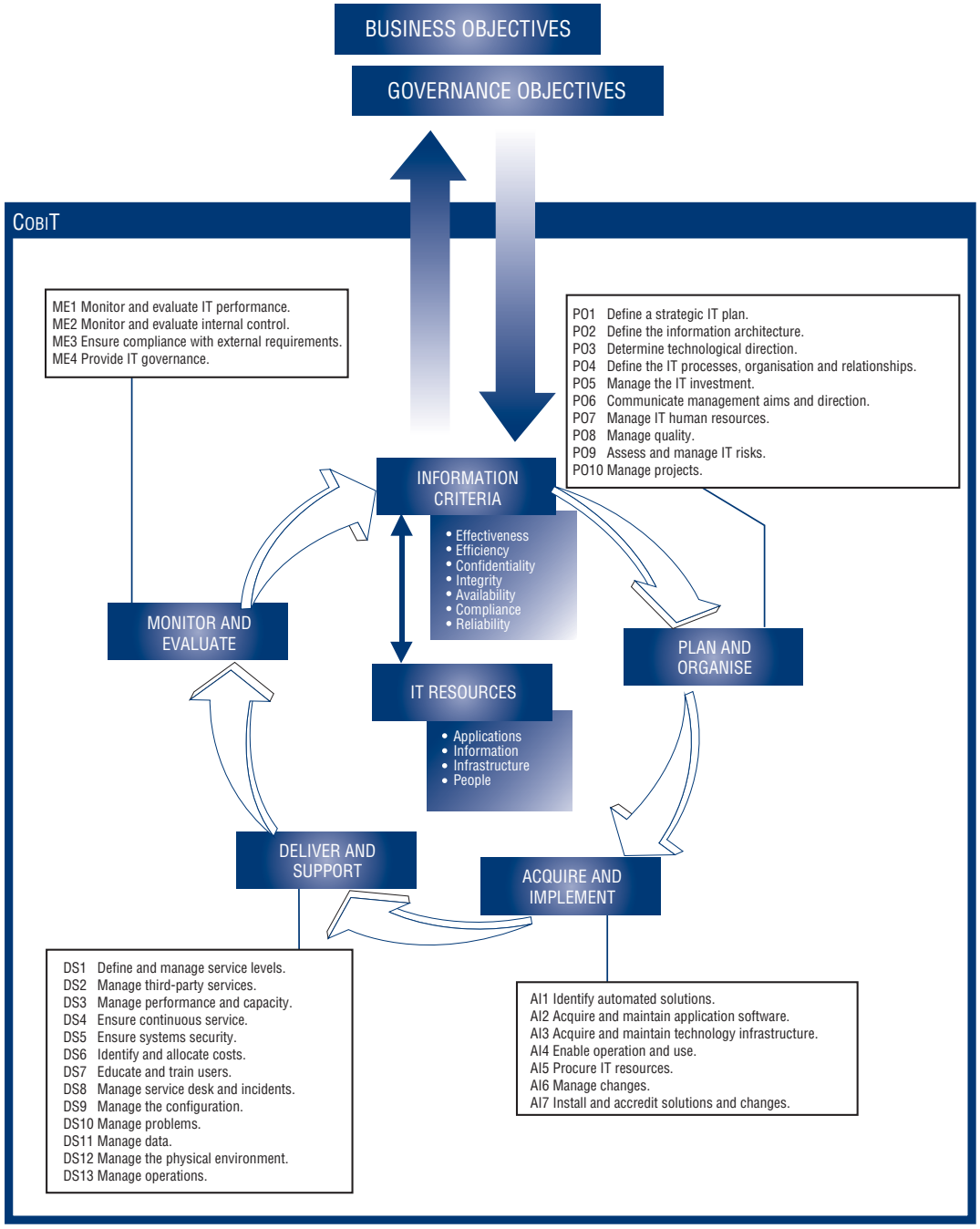
Effective controls reduce risk, increase the likelihood of value delivery, and improve efficiency because there will be fewer errors and a more consistent management approach. To achieve effective governance, controls need to be implemented by operational managers within a defined control framework for all IT processes. Since COBIT's IT control objectives are organised by IT process, the framework provides clear links amongst IT governance requirements, IT processes and IT controls. Each of COBIT's IT processes has a process description and a number of control objectives. As a whole, they are the characteristics of a well-managed process.

IT General Controls and Application Controls

General controls are controls embedded in IT processes and services. Examples include systems development, change management, security and computer operations. Controls embedded in business process applications are commonly referred to as application controls. Examples include completeness, accuracy, validity, authorisation and segregation of duties.

COBIT assumes the design and implementation of automated application controls to be the responsibility of IT, which are covered in the Acquire and Implement domain. The operational management and control responsibility for application controls is not with IT, but with the business process owner. Hence, the responsibility for application controls is an end-to-end joint responsibility between business and IT. The business is responsible to properly define functional and control requirements, and use automated services. IT is responsible to automate and implement business functional and control requirements, and establish controls to maintain the integrity of applications controls. Therefore, the COBIT IT processes cover general IT controls, but only the development aspects of application controls;

Figure 3—Overall COBIT Framework



responsibility for definition and operational usage is with the business. The following list provides a recommended set of application control objectives:

- AC1 Source Data Preparation and Authorisation—Ensure that source documents are prepared by authorised and qualified personnel, following established procedures, taking into account adequate segregation of duties regarding the origination and approval of these documents. Errors and omissions can be minimised through good input form design. Errors and irregularities must be detected so they can be reported and corrected.
- AC2 Source Data Collection and Entry—Establish that data input is performed in a timely manner by authorised and qualified staff members. Correction and resubmission of data that were erroneously input are performed without compromising original transaction authorisation levels. Where appropriate for reconstruction, original source documents should be retained for the appropriate amount of time.

- AC3 Accuracy, Completeness and Authenticity Checks—Ensure that transactions are accurate, complete and valid. Validate and edit, or send back for correction, input data as close to the point of origination as possible.
- AC4 Processing Integrity and Validity—Maintain the integrity and validity of data throughout the processing cycle. Detection of erroneous transactions should not disrupt the processing of valid transactions.
- AC5 Output Review, Reconciliation and Error Handling—Establish procedures and associated responsibilities to ensure that the necessary control information is provided and used to enable verification, detection and correction of the accuracy of output.
- AC6 Transaction Authentication and Integrity—Before passing transaction data between internal applications and business or operational functions (in or outside the enterprise), check for proper addressing, authenticity of origin and integrity of content. Maintain authenticity and integrity during transmission or transport.

Measurement-driven

A basic need for every enterprise is to understand the status of its own IT systems and to decide what level of management and control the enterprise should provide. To decide on the right level, management should ask: How far should we go, and is the cost justified by the benefit? Obtaining an objective view of an enterprise's own performance level is not easy. Enterprises need to establish goals and metrics to measure where they are and where improvement is required, and implement a management tool kit to monitor this improvement.

Goals and metrics are defined in COBIT at three levels:
- IT goals and metrics that define what the business expects from IT and how to measure it
- Process goals and metrics that define what the IT process must deliver to support IT's objectives and how to measure it
- Activity goals and metrics that establish what needs to happen inside the process to achieve the required performance and how to measure it

Goals are defined top-down in that a business goal will determine a number of IT goals to support it. An IT goal is achieved by one process or the interaction of a number of processes. Therefore, IT goals help define the different process goals. In turn, each process goal requires a number of activities, thereby establishing the activity goals.

COBIT uses two types of metrics:
- Outcome measures, previously key goal indicators (KGIs), indicate whether the goals have been met. These can be measured only after the fact and, therefore, are called 'lag indicators'.
- Performance indicators, previously key performance indicators (KPIs), indicate whether goals are likely to be met. They can be measured before the outcome is clear and, therefore, are called 'lead indicators'.

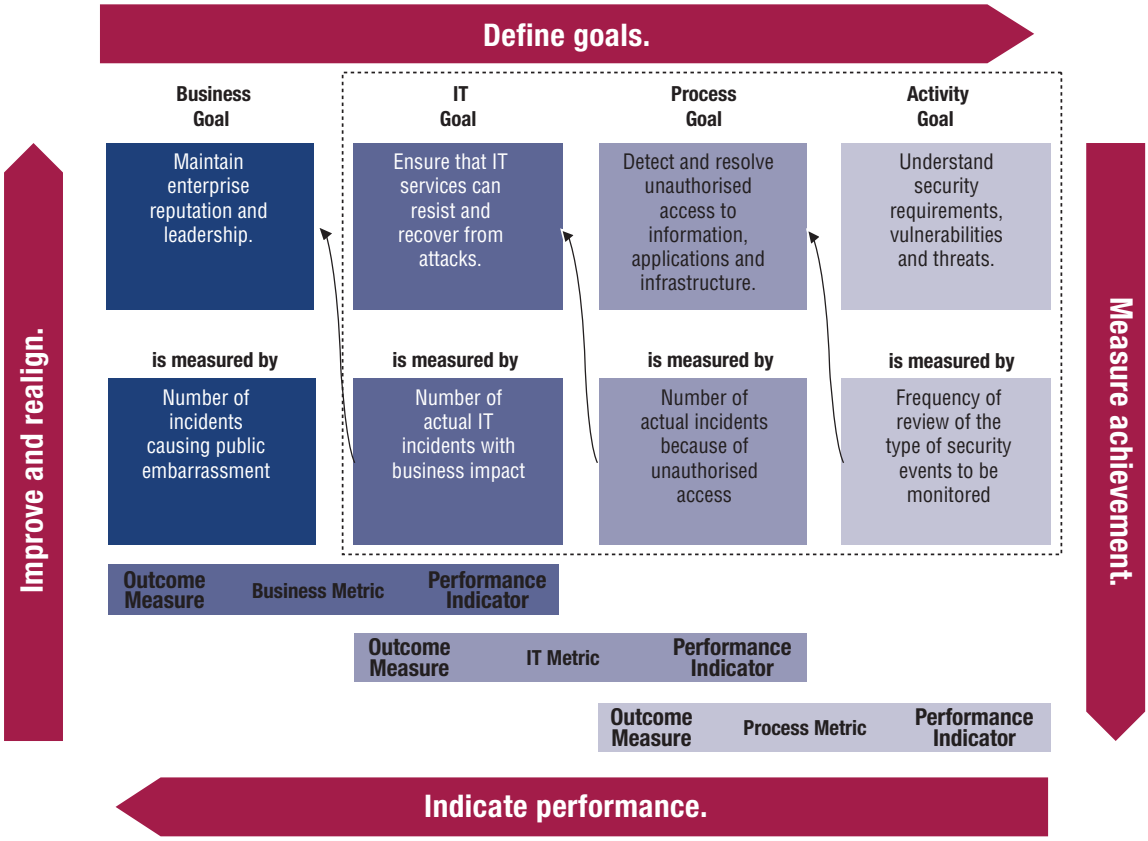
Outcome measures define measures that inform management—after the fact—whether an IT function, process or activity has achieved its goals. The outcome measures of the IT functions are often expressed in terms of information criteria:
- Availability of information needed to support the business needs
- Absence of integrity and confidentiality risks
- Cost-efficiency of processes and operations
- Confirmation of reliability, effectiveness and compliance

Performance indicators define measures that determine how well the business, IT function or IT process is performing in enabling the goals to be reached. They are lead indicators of whether goals will likely be reached, thereby driving the higher-level goals. They often measure the availability of appropriate capabilities, practices and skills, and the outcome of underlying activities. For example, a service delivered by IT is a goal for IT, but a performance indicator and a capability for the business. This is why performance indicators are sometimes referred to as performance drivers, particularly in balanced scorecards.

Therefore, the metrics provided are both an outcome measure of the IT function, IT process or activity goal they measure, and a performance indicator driving the higher-level business, IT function or IT process goal.

Figure 4 illustrates the relationship amongst the business, IT, process and activity goals, and the different metrics. From top left to top right, the goals cascade is illustrated. Below the goal is the outcome measure for the goal. The small arrow indicates that the same metric is a performance indicator for the higher-level goal.

Figure 4—Relationship Amongst Process Goals and Metrics (DS5)



CONCLUSION

COBIT is based on the analysis and harmonisation of existing IT standards and best practices and conforms to generally accepted governance principles. It is positioned at a high level, driven by business requirements, covering the full range of IT activities, and concentrating on what should be achieved rather than how to achieve effective governance, management and control. Therefore, it acts as an integrator of IT governance practices and appeals to executive management; business and IT management; governance, assurance and security professionals; and IT audit and control professionals.

COBIT is designed to be complementary to, and used together with, other standards and best practices. Implementation of best practices should be consistent with the enterprise's governance and control framework, appropriate for the organisation, and integrated with other methods and practices that are being used. Standards and best practices are not a panacea, and their effectiveness depends on how they have been implemented and kept up to date. They are most useful when applied as a set of principles and as a starting point for tailoring specific procedures.

COBIT has been developed and is maintained by an independent, not-for-profit research institute, drawing on the expertise of its affiliated association's members, industry experts, and control and security professionals. Its content is based on continuous research into IT best practice and is continuously maintained, providing an objective and practical resource for all types of users.

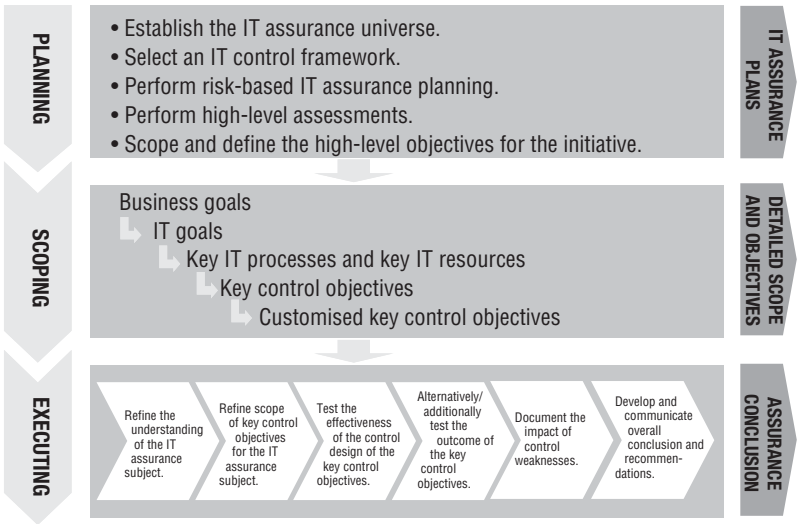
4. PROVIDING IT ASSURANCE

The objective of an assurance initiative is for an assurance professional to measure or evaluate a process that is the responsibility of another party. For IT assurance initiatives, there is generally also a stakeholder involved who benefits from the process, but who has delegated operation and custodianship of the process to another party. Hence, the stakeholder is the end customer of the evaluation.

To provide assurance, it is important to follow a consistent methodology or approach. While the specific approach may be unique to each organisation and type of initiative, a fairly similar approach will be used across all assurance initiatives. Assurance is provided in three stages:
- Planning
- Scoping
- Execution

The stages and specific steps performed during each stage are illustrated in the IT assurance road map presented in **figure 5**.
It is important to understand that, historically, IT assurance started in support of financial statement audits. The purpose of a financial audit is, typically, to express an opinion on financial statements. The minimum requirement for the assurance professional is to

Figure 5—IT Assurance Road Map



understand the information systems underpinning business processes relevant for financial reporting and how the entity has responded to risks arising from IT. Since the use of IT affects the way control activities are implemented in the business and related financial reporting, the assurance professional needs to consider whether the entity has responded adequately to the risks arising from IT by establishing effective general IT controls and application controls.

Planning is the first stage on the IT assurance road map. To create a comprehensive plan, the assurance professional needs to combine an understanding of the IT assurance universe and the selection of an appropriate IT control framework such as COBIT. The aggregation of these two will allow for risk-based planning of the assurance initiative. The end deliverable of this stage is the IT assurance plan.

Scoping is the second stage on the IT assurance road map. Scoping begins with defining business and IT goals for the environment under review, and identifying a set of IT processes and resources (i.e., assurance universe) required to support those goals. These goals can be scoped down to a lower granularity, i.e., key control objectives customised for the organisation, which are subject to the IT assurance initiative. The end deliverables of this stage are the scope and objectives of the different IT assurance initiatives.

Execution is the third stage on the IT assurance road map. Execution involves performing the core testing activities. The end deliverable of this stage is the conclusion of the IT assurance initiative.

ASSURANCE PLANNING

Before beginning an assurance initiative, the work of the IT assurance professional should be planned in a manner appropriate for meeting the assurance objectives. For an internal assurance function, the assurance plan should be developed, then updated and reviewed at least annually. The plan should act as a framework for assurance activities and address responsibilities set by the organisation's assurance charter. For an external IT assurance initiative, a plan should normally be prepared for each initiative. Each type of assurance plan should clearly document the objectives of the initiative and reflect management's strategy and priorities.

As part of the planning process, IT assurance professionals should obtain an understanding of the assurance universe, including the organisation's:
- Business goals for IT
- IT goals and how they are planned to be realised through IT processes
- IT resources

The IT resources are defined as follows:
- Applications are the automated user systems and manual procedures that process the information.
- Information is the data input, processed and output by the information systems, in whatever form is used by the business.
- Infrastructure is the technology and facilities (hardware, operating systems, database management systems, networking, multimedia, etc., and the environment that houses and supports them) that enable the processing of the applications.
- People are the personnel required to plan, organise, acquire, implement, deliver, support, monitor and evaluate the information systems and services. They may be internal, outsourced or contracted as required.

The extent of the knowledge required is determined by the nature of the organisation, its environment and risks, and the objectives of the assurance initiative. To execute the assurance initiative and assurance planning work according to a standardised and structured approach, the IT assurance professional should also identify appropriate control frameworks that could be useful for developing assurance initiatives.

The portfolio of assurance activities within the assurance universe needs to be prioritised by risk level, technological complexity, time since the most recent assurance initiative and strategic importance. By doing so, assurance resources can be assigned to the units carrying the highest risk for the organisation. It helps to think in terms of IT resources for translating business goals into IT goals, i.e., in terms of the services and information required, and in terms of the infrastructure and people resources required to provide and support the services and information needed.

The assurance professional should use an appropriate risk assessment technique or approach in developing the overall plan for the effective allocation of IT assurance resources. Risk assessment is a technique used to examine units in the assurance universe and select those areas for review that have the greatest risk exposure. The risks associated with each IT layer cannot be determined by reviewing the IT-related risks in isolation, but must be considered in conjunction with the organisation's processes and objectives.

The suggested risk analysis approach starts from the valuation of assets, which, in the COBIT framework, consists of the information that has the required criteria to help achieve the business objectives (including all the resources necessary to produce that information). The next step is the vulnerability analysis, which identifies the vulnerabilities that apply to the assets, e.g., a business process that needs to comply with data privacy, a business product that deals with financial transactions or infrastructure elements that determine the availability of many information services. The next phase identifies significant threats that may be able to exploit a given vulnerability, e.g., unintentional events, such as errors, omissions and accidents, or intentional actions, such as fraud, hacking or theft.

The probability of the threat, the degree of vulnerability and the severity of the impact are combined to develop threat/vulnerability scenarios and assess their risk. This is followed by the selection of countermeasures (controls) and an evaluation of their cost and effectiveness. After considering the impact of implementing selected controls, residual risk can be determined. The conclusion is an action plan after which the cycle can start again.

DEFINING THE SCOPE OF THE ASSURANCE INITIATIVE

The scoping stage determines which IT resources and control objectives will be covered, and consists of linking applicable IT resources (information, applications, infrastructure, people) to applicable IT control objectives, and then assessing the materiality of the impact of not achieving a specific control objective. Setting the scope for the initiative too narrowly may result in material factors not being

considered. Setting the scope for the initiative too broadly may result in inefficiencies and incorrect conclusions because of limited resources and time.

IT assurance professionals should clearly define the scope and objectives of the assurance work by performing a preliminary assessment of internal control of the activities being reviewed to provide reasonable assurance that all material items will be adequately covered during the assurance initiative. There are eight steps in scoping IT resources and control objectives.

1. **Establish drivers for the assurance initiative.** There are many possible drivers for assurance, including process improvement and meeting compliance needs in support of the financial statement audit. Verifying the drivers for the assurance initiative can be accomplished by activities such as interviewing key stakeholders or inspecting assurance plans or charters. More specifically, the boundaries of the entity under review need to be unambiguously described, together with the current roles and responsibilities and the resources required by IT to support the defined business needs of the entity under review.
2. **Document the enterprise IT architecture.** The concept and elements of the architecture can be validated by interviews with key IT staff members.
3. **Select control frameworks.** Typically this will be COBIT, but for some initiatives it may be COSO, similar entity-level control frameworks, or more detailed frameworks or standards, such as one of the relevant ISO standards.
4. **Identify IT processes.** After selecting the appropriate control framework, the appropriate IT processes must be selected. IT processes in scope can be identified through analysis of the relationship amongst business goals, IT goals and IT processes.
5. **Link IT processes to IT resources.** IT resources are made up of applications, information, infrastructure and people. A number of inputs can be used to determine the IT resources that are relevant to the initiative. The priority here should be on completeness because the subsequent risk analysis will determine items that can be excluded from the scope of the initiative. The different inputs are the following:
   – Drivers for the initiative are the most important factors for determining the IT components and the control objectives to review. Typical examples are major service breakdown, organisational change and regulatory compliance.
   – Business control requirements are identified by analysing the required and applicable business controls so that the scoping of IT controls is limited to how IT supports automated business controls.
   – Enterprise architecture for IT encompasses the processes involved to deliver the information services, the portfolio of applications and systems in use by the organisation; the technology used to run them; and the people needed to plan, build, operate and support the applications. The relevant IT resources or groups of IT resources can be deduced from the architecture.
6. **Refine IT resources.** In the initial linking of processes to resources, the assurance professional may derive a rather large portfolio, perhaps broader than can be cost-effectively reviewed within the terms of the assurance initiative. In this step, the assurance professional should refine the selection of IT resources by ensuring that the resources have a direct relationship to the processes relevant to the initiative.
7. **Select control objectives.** The assurance professional makes a first selection of the control objectives that are relevant for the IT processes that are in scope for the assurance initiative. It will often be necessary to customise the control objectives for the realities of the particular enterprise situation. For most initiatives, scoping IT resources does not require substantial analysis because it starts from a specific enterprise situation. Conversely, scoping the control objectives needs more analysis because it starts from one or more generic frameworks.
8. **Refine match of control objectives and IT resources.** The assurance professional links the refined portfolio of IT resources set out in step six to the first cut of control objectives selected in the seventh step. In an iterative process, the professional refines and often reduces the list of control objectives that are relevant for this particular assurance initiative.

During the last step, the assurance professional should analyse the risk of not achieving the selected control objectives for the selected IT resources, and only retain the IT resources and control objectives that have a material effect if the control objective is not achieved. The assurance professional should determine if there is sufficient risk to keep the IT resource in scope, and remove the control objectives that are low risk. The critical conclusion of this step is to answer the following question: Will not achieving this control objective for this class of IT resource be material for this particular assurance initiative? Only the cells for which the answer is 'yes' will be retained in the final IT control scope.

ASSURANCE INITIATIVE EXECUTION

The assurance steps to be performed determine the scope of the assurance project. The assurance scope and objectives need to be communicated to and agreed upon by all stakeholders. The output from this step will consist of the documented evidence for:

- Who performs the task(s), where the task is performed and when the task is performed
- The inputs required to perform the task and the outputs generated by the task
- The stated procedures for performing the task

Refine Understanding of the Environment

The first step of the execution stage is refining an understanding of the environment in which the testing will be performed. This implies understanding the organisation to select the correct assurance scope and objectives. Scope is determined by selecting a subset of the assurance universe (i.e., process, system, application) on one hand and a set of controls to be reviewed on the other hand. To align the assurance objectives and approach to the business objectives, it is necessary to understand the related business processes, the business goals, and the relevance of IT to the processes and objectives. The IT goals need to be defined, bearing in mind the assurance requirements and the IT organisation.

The assurance provider must identify the in-scope IT processes, IT control objectives and IT resources to establish the assurance boundaries. The identification of the processes, objectives and related resources is performed by assessing if it is likely that non-achievement of the control objective for the IT component will have a material effect. The inherent risk of material control objectives not being met determines the amount of assurance review and testing required.

Refining understanding of the environment provides a basis for setting the assurance strategy and refining the scope of the assurance initiative based on the assessed risk. The assurance provider can now adjust the IT processes, IT resources and IT control objectives that will be selected for testing; determine what documentation is required; and develop a testing approach that ensures the most effective and efficient coverage of assurance objectives.

Testing the Control Design

Testing is performed to evaluate the design of the controls, confirm that controls have been placed in operation and assess the operational effectiveness of the control. Different types of testing can be applied, which include the following generic testing methods:

- Enquire and confirm:
  - Search for exceptions/deviations and examine them.
  - Investigate unusual or non-routine transactions/events.
  - Check/determine whether something has (not) occurred (sample).
  - Corroborate management statements from independent sources.
  - Interview staff members and assess their knowledge and awareness.
  - Reconcile transactions (e.g., reconciling transactions to bank statements).
  - Ask management questions and obtain answers to confirm findings.
- Inspect:
  - Review plans, policies and procedures.
  - Search audit trails, problem logs, etc.
  - Trace transactions through the process/system.
  - Physically inspect presence (documentation, assets, etc.).
  - Walk through installations, plans, etc.
  - Perform a design or code walk-through.
  - Compare actual with expected findings.
- Observe:
  - Observe and describe the processes.
  - Observe and describe the procedures.
  - Compare actual with expected behaviour.
- Reperform and/or recalculate:
  - Independently develop and estimate the expected outcome.
  - Attempt what is prevented.
  - Reperform what is detected by detective controls.
  - Reperform transactions, control procedures, etc.
  - Recalculate independently.
  - Compare expected value with actual value.
  - Compare actual with expected behaviour.
  - Trace transactions through the process/system.
- Automated evidence collection:
  - Collect sample data.
  - Use embedded audit modules.
  - Analyse data using computer-assisted audit techniques (CAATs).
  - Extract exceptions or key transactions.

To assess the adequacy of the design of controls, the assurance provider should:
- Observe or inspect and review the control approach, and test the design for completeness, relevancy, timeliness and measurability.
- Enquire and confirm whether responsibilities for the control practices and overall accountability have been assigned, test whether accountability and responsibilities are understood and accepted, and verify that the right skills and the necessary resources are available.
- Enquire through interviews with key staff members involved whether the control mechanism, its purpose, and the accountability and responsibilities are understood.

In summary, the assurance professional must determine whether:
- Documented control processes exist
- Appropriate evidence of control processes exists
- Responsibility and accountability are clear and effective
- Compensating controls exist, where necessary, to mitigate weakness in related controls

Testing the Control Outcome

The assurance steps to be performed ensure that the control measures established are consistently and continuously working as prescribed, and conclude on the appropriateness of the control environment. To test the outcome or effectiveness of the control, the assurance professional needs to look for direct and indirect evidence of the control's impact on the quality of the process outputs. This implies the direct and indirect substantiation of measurable contribution of the control to the IT, process and activity goals.

The assurance professional should obtain evidence for selected items and periods to ensure that the control under review is working effectively by applying various testing techniques. The assurance professional should also perform a limited review of the adequacy of the process deliverables and determine the level of substantive testing needed to provide assurance that the IT process is performing as intended.

Document Impact of Control Weaknesses

When control weaknesses are found, they have to be properly documented, taking into account their often sensitive and confidential nature. In addition, particular care is required to correctly assess the severity of the observed weaknesses and the potential business impact that weakness may have. The objective of this step is to conduct the necessary testing to provide management with assurance (or nonassurance) about the achievement of a given business process and related control objectives. More detailed analysis should occur when no control measures are in place, controls are not working as expected or controls are not consistently applied. This should result in a thorough understanding of the control weaknesses and the resulting threats and vulnerabilities, and in an understanding of the potential impact of the control weaknesses.

Assurance steps to be performed to document the impact of not achieving the control objective include the following:
- Relate to actual cases in the same industry, and leverage industry benchmarks.
- Link known performance indicators to known outcomes and, in their absence, link cause to effect (cause/effect analysis).
- Illustrate where the impact is (e.g., on business goals and objectives, on enterprise architecture elements, on capabilities and resources).
- Illustrate the impact of control weaknesses with numbers and scenarios of errors, inefficiencies and misuse.
- Clarify vulnerabilities and threats that are more likely with controls not operating effectively.
- Document impact of actual control weaknesses in terms of bottom-line impact, integrity of financial reporting, hours lost in staff time, loss of sales, ability to manage and react to market, customer and shareholder requirements, etc.
- Point out consequences of non-compliance with regulatory requirements and contractual agreements.
- Measure the actual impact of disruptions and outages on business processes and objectives, and on customers (number, effort, downtime, customer satisfaction, cost).
- Document the cost (customer and financial impact) of errors that could have been caught by effective controls.
- Measure and document cost of rework, e.g., the ratio of rework to normal work, as an efficiency measure affected by control weaknesses.
- Measure actual business benefits and illustrate cost savings of effective controls after the fact.
- Use benchmarking and survey results to compare the enterprise performance with others.
- Extensively use graphics to illustrate the issues.

Develop and Report Overall Conclusion and Recommendations

The substantiated risk of the control weaknesses must be communicated to the different stakeholders of the assurance initiative. The assurance professional should document any identified control weaknesses and resulting threats and vulnerabilities, and identify and document the actual and potential impact. In addition, the assurance professional may provide comparative information, e.g., through benchmarks, to establish a reference framework in which the test results ought to be evaluated. The objective is to identify items of significance to be able to articulate to the stakeholder the recommended actions and reasons for taking action.

This phase includes aggregating the results of the previous phases, developing a conclusion concerning the identified control weaknesses and communicating:
- Recommended actions to mitigate the impact of the control weaknesses
- Performance comparison to standards and best practices for a relative view on the results
- The risk associated with a failure to perform the process effectively

The formulated conclusion and recommendations should allow the responsible party to take further steps and remedial actions. When the assurance initiative is performed within an assurance context, the assurance professional needs to be thoughtful of formal assurance communication and compliant with assurance reporting standards and guidelines.

EXAMPLES OF THE USE OF DETAILED ASSURANCE STEPS

The following sections provide illustrative examples of how the assurance testing steps could be applied.

Testing of Control Design

Situation: General computer controls review in a transaction processing organisation; assessment of the COBIT process AI6 Manage Changes; COBIT control objective *AI6.2 Impact assessment, prioritisation and authorisation*

Observations: For the selected systems (e.g., application, platform or network), the assurance professional inventoried the types of changes that can be implemented, procedures (formal or informal) currently in place, all parties involved in the change management process, tools used, etc. This was done through interviews with involved persons and enquiries for documented procedures. The result of this work was a comprehensive and correct flowchart of the change management process.

The assurance professional reviewed the identified process flow to determine whether there was a step defined in the procedure to assess the impact of a change by a competent person or group of persons. The assurance professional observed that the template for requesting and approving changes included a section on impact assessment. However, the change management procedure did not mention that this information is mandatory, and the absence of this information did not lead to a rejection of the change request. In addition, the procedure did not mention any documentation standards or required verification and approval steps for the impact assessment.

Test Result: The design of this control is flawed, because a fundamental component of the control, i.e., impact assessment, is incomplete at best. It is possible that changes are implemented without proper risk assessment, which can lead to unplanned and difficult-to-contain operational disruptions or malfunctions.

Testing for the Effectiveness of the Control

Situation: General computer controls review in a transaction processing organisation; assessment of the COBIT process AI6 Manage Changes; COBIT control objective *AI6.3 Emergency changes*

Observations: As part of the evaluation of the control design, the assurance professional identified that, for all relevant change management procedures, there is a control defined to help ensure that emergency change requests are reintroduced into the normal change management cycle. In addition, the assurance professional found that there is a procedure that ensures that all emergency changes are appropriately logged in a change management tool.

As part of the control effectiveness testing, a sample of emergency change requests was selected from the change management tool and traced to their reintroduction as normal changes. This tracing included verification of whether the emergency change was actually introduced again as a normal change and whether it was processed following the normal change management procedure.

The assurance professional observed that from the sample of 25 emergency changes selected, three were not subsequently reprocessed as normal changes. In addition, the assurance professional found that from the 22 emergency changes that had been duly reintroduced, only 10 were discussed at the change management board—or at least that there was a trace available that indicated that the 10 changes were discussed (trace included information stored in the change management tool).

Test Result: The emergency change procedure is not effective for two reasons:

- Not all emergency changes are reintroduced in the system, leading to a risk of losing emergency changes from sight and not learning from them.
- Emergency changes that have been reintroduced are most likely inadequately discussed and documented, leading to the same risk.

Documenting the Impact of Control Weaknesses

Situation: General computer controls review in a transaction processing organisation; assessment of the COBIT process AI6 Manage Changes; COBIT control objective *AI6.3 Emergency changes*

Observations: Using the situation as described, the assurance professional needed to gain additional information and perform further analysis to assess and document the impact of the control weaknesses. For the aforementioned examples, the assurance professional needed to consider the types and numbers of changes affected by the control weaknesses.

Some of the required information might/should already be gathered at the planning stage. This information should be used to evaluate the materiality of the weaknesses noted. Notably, the changes affected should be mapped back to the relevant infrastructure components and the applications/information they support/process. In addition, SLA penalties might apply. Analysis of problems noted in the past can help establish the real potential impact of the weaknesses noted.

In this case, it turns out, after discussion with the responsible change manager and confirmation with other change management board members, that the missing emergency changes relate to non-critical systems, and that the missing documentation was only a documentation issue, whereas the actual change, its cause and consequences had, indeed, been discussed but were not formally documented.

Test Result: Although the control weaknesses remain as they have been observed, further analysis and documentation showed that the weaknesses were of a lesser importance than originally assessed.

CONCLUSION

An assurance initiative involves three phases. First, the assurance professional must develop a plan that identifies the assurance universe and uses an appropriate IT control framework to identify the assurance objectives based on a high-level risk assessment. Second, the initiative must be scoped through a top-down analysis that identifies the business goals to be examined and the IT goals that support those business goals, then identifies the IT processes and resources necessary to accomplish the IT goals and the key control objectives that must be accomplished for those processes to function effectively. Third, the initiative must be executed by refining understanding of the key control objectives within the assurance universe, evaluating the design and operational effectiveness of control procedures that address key control objectives, evaluating the impact of any deficiencies that come to light, and communicating findings and recommendations to stakeholders.

5. AUDITING IT CONTROLS OVER FINANCIAL REPORTING

In today's environment, financial reporting processes are driven by IT systems. Such systems, whether ERP or otherwise, are deeply integrated in initiating, authorising, recording, processing and reporting financial transactions. As such, they are inextricably linked to the overall financial reporting process and need to be assessed along with other important processes.

In understanding where IT controls exist within the typical company, consideration should be given to at least three elements. First, executive management establishes and incorporates strategy into business activities. From an IT perspective, policies and other enterprisewide guidelines are set and communicated throughout the organisation. Second, business processes are the organisation's mechanism of creating and delivering value to its stakeholders. Increasingly, business processes are being automated and integrated with complex and highly efficient IT systems. Third, IT services form the foundation for operations and are provided across the organisation, rather than segregated by business process or business unit.

More and more, IT systems are automating business processes. In doing so, these systems often replace manual control activities with automated or IT-dependent control activities. As a result, compliance programs need to consider system-based controls to keep pace with changes in business processes and new system functionality. Whether through a unified ERP system or a disparate collection of operational and financial management software applications, IT is the foundation of an effective system of internal control over financial reporting. IT controls commonly include controls over the IT environment, computer operations, access to programs and data, program development, and program changes.

IT CONTROL ENVIRONMENT

The IT control environment includes the IT governance process. The IT governance process includes the information systems strategic plan; the IT risk management process; compliance and regulatory management; and IT policies, procedures and standards. Monitoring and reporting are required to align IT with business requirements. The IT governance structure should be designed so that IT adds value to the business and IT risks are mitigated. This also includes an IT organisation structure that supports adequate segregation of duties and promotes the achievement of the organisation's objectives.

COMPUTER OPERATIONS

These include controls over the definition, acquisition, installation, configuration, integration and maintenance of the IT infrastructure. Ongoing controls over operations address the day-to-day delivery of information services, including service-level management, management of third-party services, system availability, customer relationship management, configuration and systems management, problem and incident management, operations management scheduling, and facilities management.

The system software component of operations includes controls over the effective acquisition, implementation, configuration and maintenance of operating system software, database management systems, middleware software, communications software, security software and utilities that run the system and allow applications to function. System software also provides the incident tracking, system logging and monitoring functions. It can report on uses of utilities, so if someone accesses these powerful data-altering functions, at least that individual's use is recorded and reported for review.

ACCESS TO PROGRAMS AND DATA

Access controls over programs and data assume greater importance as internal and external connectivity to entity networks grows. Internal users may be halfway around the world or down the hall, and there may be thousands of external users accessing, or trying to access, entity systems. Effective access security controls can provide a reasonable level of assurance against inappropriate access and unauthorised use of systems. If designed well, they can intercept unethical hackers, malicious software and other intrusion attempts.

Adequate access control activities, such as secure passwords, Internet firewalls, data encryption and cryptographic keys, can be effective methods of preventing unauthorised access. User accounts and related access privilege controls restrict the applications or application functions only to authorised users who need them to do their jobs, supporting an appropriate division of duties. There should be frequent and timely review of the user profiles that permit or restrict access. Former or disgruntled employees can be a threat to a system; therefore, terminated employee passwords and user IDs should be revoked immediately. By preventing unauthorised use of, and changes to, the system, an entity protects its data and program integrity.

PROGRAM DEVELOPMENT AND PROGRAM CHANGE

Application software development and maintenance have two principal components: the acquisition and implementation of new applications and the maintenance of existing applications. The acquisition and implementation process for new applications tends to result in a high degree of failure. Many implementations are considered to be outright failures, as they do not fully meet business requirements and expectations, or are not implemented on time or within budget.

To reduce acquisition and implementation risks, some entities have a form of system development and quality assurance methodology. Standard software tools and IT architecture components often support this methodology. The methodology provides structure for the identification of automated solutions, system design and implementation, documentation requirements, testing, approvals, project management and oversight requirements, and project risk assessments.

Application maintenance addresses ongoing change management and the implementation of new releases of software. Appropriate controls over changes to the system should exist so that all changes are made properly. There is also a need to determine the extent of testing required for the new release of a system. For example, the implementation of a major new software release may require the evaluation of enhancements to the system, extensive testing, user retraining and the rewriting of procedures.

Controls may involve required authorisation of change requests, review of the changes, approvals, documentation, testing and assessment of changes on other IT components, and implementation protocols. The change management process also needs to be integrated with other IT processes, including incident management, problem management, availability management and infrastructure change control.

THE AUDIT PROCESS

Auditing IT controls over financial reporting involves the following six interdependent processes:
1. Plan and scope IT controls
2. Assess IT risk
3. Document controls
4. Evaluate control design and operating effectiveness
5. Prioritise and remediate deficiencies
6. Build sustainability

1. Plan and Scope IT Controls

Like all significant projects, careful attention should be given to properly scoping and planning the IT compliance program. Planning is the process of developing a time schedule of activities whereby tasks are assigned to people and progress can be monitored. Scoping is the process of understanding which IT applications and related subsystems should be included in the project and which applications and subsystems can be excluded, based on the results of the overall financial risk assessment. In other words, only the applications and related subsystems that support business and relevant controls over financial reporting should be included in scope.

Assign Accountability and Responsibility
An important first step in the IT control compliance program is to form an audit team. The audit team should be integrated into, and report to, the IT steering committee. Smaller organisations may be able to redeploy, on a part-time basis, existing staff members; however, larger organisations may need dedicated full-time personnel. The subcommittee should assign an IT controls lead who is responsible for the project and is given appropriate authority and accountability for completing the project.

Inventory Relevant Applications and Related Subsystems
An inventory of in-scope applications should be developed by identifying the applications that support relevant application controls. Typically, applications that support online authorisations, complex calculations or valuations, or are responsible for maintaining the integrity of significant account balances, such as inventory, fixed assets or loan balances, should be identified in this phase. By having an inventory of applications, as well as the IT processes that manage and drive the applications, the audit team will be able to identify all applications that need to be considered and identify all subsystems that support the applications.

Organisations have many business processes and controls that support financial reporting. Consequently, it is important that the audit team participate in the identification of application controls. In doing so, organisations are able to properly plan the IT controls project, limiting scope to application controls that support financial reporting objectives.

Develop a Preliminary Project Plan and Obtain Approval
Using the inventory of in-scope applications and subsystems, a preliminary project plan of activities should be developed using the phases described in **figure 5**. The project plan will be modified and refined later, but it is important to get an overall view of the project's size and approach. Once the plan is developed, it is important to evaluate the in-scope applications and appropriateness of the project's scope. When this is complete, it is time to obtain approval to proceed with the project. Obtaining formal approval is very important given the significance of the project and the impact it will have on various members of the organisation. Formal approval will solidify the sponsors of the project and allow one to obtain buy-in from all relevant stakeholders and staff members who need to participate.

Determine Responsibility for Application Controls
One of the common areas of confusion for IT control projects has been 'who is responsible for application controls?' The lack of clarification of this responsibility has led to significant duplication of effort, unnecessary testing of duplicative relevant controls and the risk that a relevant control may not be tested. It is suggested that business owners are responsible for business-process-specific application controls. The responsibility of the IT organisation is to assist the process owners in identifying and testing these controls, whilst ensuring that the general application controls (access restrictions, change controls, backup recovery, etc.) are in place and reliable.

Consider Multilocation Issues
Amongst the many factors that should be considered in scoping the IT control project are companies with decentralised operations or companies with operations that span geographic boundaries. Such companies need to determine if their IT operations in each geographic location operate within a single control environment or multiple control environments. Single control environments typically have one leadership structure, whilst multilocation environments typically have multiple leadership structures. Generally speaking, multilocation environments, when significant, have to be treated separately and, therefore, result in a larger project and more work.

Consider Whether Applications Can Be Eliminated From Scope
The fact that an application is included in scope indicates that it supports a relevant application or hybrid control. In most cases, the application and its related subsystems will have to be assessed. However, if the application supports a very limited number of application controls (e.g., just one control), consideration could be given to eliminating the application control (and, therefore, the application itself) and either identifying a relevant manual control or increasing reliance on existing manual controls to reduce overall effort. Whilst this is rare, it is a consideration for companies that have many applications that support very few controls. Care should be taken to ensure that inadvertent reliance does not occur in these situations (e.g., relying on a system-generated report).

Identify Dependencies on Third-party Service Organisations (Outsourcing)
Some organisations use external service organisations to perform outsourced services. These services are still part of an organisation's overall operations and responsibility and, consequently, need to be considered in the overall IT internal control program. The use of a service organisation does not reduce management's responsibility to maintain effective internal control over financial reporting. Rather, management should evaluate controls at the service organisation, as well as related controls at the company, when making its assessment about internal control over financial reporting.

Organisations should review the activities of the service organisation in arriving at a conclusion on the reliability of its internal control. Documentation of service organisation control activities will be required for the attestation activities of the independent auditor. Therefore, an assessment is required of the service organisation to determine the sufficiency and appropriateness of evidence supporting these controls.

2. Assess IT Risk

At this point, organisations need to assess risks within the IT processes and layers that support the applications in scope. One of the most significant lessons learned through the initial years of Sarbanes-Oxley compliance projects is that the project needs to be risk-based. Not all IT systems or processes pose a high risk to the financial statements and, therefore, not all IT systems or processes need to be included or evaluated to the same extent. In performing a risk assessment, consideration needs to be given to inherent risk rather than residual risk (the risk left over after considering the impact of controls).

Assess the Inherent Risk of Applications and Related Subsystems
Assessing inherent risk of applications and their related subsystems, such as databases, operating systems, networks and physical environments, is necessary to determine the nature and extent of controls needed to manage such risks. It is also necessary to understand application and related subsystem inherent risk to properly plan and perform testing of operating effectiveness of such controls. In performing an inherent risk assessment, consideration should be given to a number of risk factors; however, the final assessment is judgemental. The purpose of considering common risk factors is to provide companies with relevant information so that a fair and reasonable risk assessment can be made.

In performing the risk assessment, both the probability and impact of the risk event should be taken into consideration. For example, without access controls, there is a risk that someone could access the primary financial application and enter false transactions into the system. Without controls, the likelihood of this happening is not entirely remote and the impact of entering false transactions is significant. As a result, this risk is considered significant and controls are required to reduce the risk. It is important to note that the objective is to reduce risk to a reasonable level, rather than eliminate risk altogether. The following factors are commonly used in performing the risk assessment, but companies should determine if others need to be added based on their unique circumstances:
- Nature of technology (complex or simple)
- Nature of people (experienced or inexperienced)
- Nature of processes (centralised or decentralised)
- Past experience
- Significance to the financial reports

Once a risk assessment has been performed, its results can assist in determining the nature and extent of controls and testing required. Regardless of the outcome, documentation of the decisions made and rationale for such decisions should be maintained for discussion with management or the external auditors.

Refine Scope and Update the Project Plan
Once a risk assessment has been performed, the audit team should be in a position to refine the project scope and update which applications and related subsystems may be excluded from scope. The risk assessment process and related conclusions should be clearly documented, particularly where systems are excluded from scope. Similarly, the project plan should be updated where changes to scope and the extent of effort is modified to reflect a risk-based approach.

3. Document Controls

Documenting controls illustrates to management how risks associated with reliable financial reporting have been addressed and enables management to make informed decisions regarding the acceptability of the remaining level of risk. For example, if financial applications are heavily relied upon for complex calculations, there is a risk that unauthorised changes could result in material errors in the financial statements. As a result, it is critical to identify and document controls that prevent this from occurring or detect its occurrence.

Identify IT Entity-level Controls
Entity-level controls are reflected in the operating style of an organisation. They include policies, procedures and other high-level practices that set the tone for the organisation. Identification of IT entity-level controls should be integrated into the overall entity-level assessment performed for the company. The existence of strong IT entity-level controls, such as well-defined and communicated policies and procedures, often suggests a more reliable IT operating environment. Similarly, organisations with weak IT entity-level controls are more likely to experience difficulty in consistently performing control activities, such as change management and access control. As a result, the relative strength or weakness of entity-level controls will impact the nature, extent and timing of testing activities.

Identify Application Controls
Identification of application controls that support financial reporting is a critical step in the process. Once all application controls have been identified, their supporting IT general controls can be identified as well. Most often, application controls are included in the business process documentation. Ideally, IT specialists document a process with a controls specialist and together they may identify the relevant controls for the process. However, in many cases, the process documentation has already been created. Therefore, someone has to review this documentation and identify the application controls. Two types of application controls are commonly used by companies and need to be documented:
- Automated controls—Performed by computers and binary in nature, they function as designed and are not subject to intermittent error. Examples include input edit checks to validate order quantities, or configured controls in automated purchasing systems to allow orders only up to preconfigured limits.
- IT-dependent manual controls (hybrid)—These are essentially manual controls that are dependent on IT systems.

IT application controls are becoming more important as the timing of error detection and the cost efficiency of controls receive more attention. For example, whereas years ago it may have been acceptable to wait several weeks for a manual reconciliation to detect an error or fraud, such a delay is becoming increasingly less acceptable. Therefore, manual controls unsupported by an automated process may no longer be tolerable.

Identify IT General Controls
Although IT general control deficiencies do not result in financial statement misstatements directly, an associated ineffective application control may lead to misstatements. Therefore, the significance of an IT general control deficiency should be evaluated in relation to its effect on application controls, that is, whether the associated application controls are ineffective. The relationship between application controls and IT general controls is such that IT general controls are needed to support the reliability of application controls.

For example, ensuring database security is often considered a requirement for reliable financial reporting. Without security at the database level, companies would be exposed to unauthorised changes to financial data. IT general controls have a pervasive effect over all internal controls. That is, if a relevant IT general control fails (e.g., a control restricting access to programs and data), it has a pervasive impact on all systems that rely on it, including financial applications. As a result, without being assured that only authorised users have access to financial applications, companies are unable to conclude that only authorised users initiated and approved transactions.

Identify Which Controls Are Relevant Controls
Financial risks are not all equal in likelihood and materiality. Similarly, financial controls are also not the same in their effectiveness in mitigating identified risks. Furthermore, management is not required to evaluate all control activities related to a risk. As a result, companies should endeavor to limit their documentation of controls to relevant controls.

The question most companies ask is 'What is a relevant control?' Unfortunately, there is no authoritative definition for relevant controls, despite the fact that the term is used ubiquitously. Whilst they may sound elusive, relevant controls are those that companies choose to rely on to meet a control objective—they are the controls that provide the most assurance to the control owners that the financial control objective was met. When judging whether a control is relevant, companies should consider the following:
- Relevant controls commonly include policies, procedures, practices and an organisation structure that are essential for management to mitigate significant risks and achieve the related control objective.
- Relevant controls often support more than one control objective. For instance, access controls support the existence of financial transactions, valuation of financial accounts, segregation of duties and more. In most cases, a combination of relevant controls is an effective way to achieve a particular objective or series of objectives. Placing too much reliance on a single control could create a single point of failure for the compliance program.
- Controls that directly address significant risks (or directly achieve objectives) are often relevant. For example, the risk of unauthorised access is a significant risk for most companies; therefore, security controls that prevent or detect unauthorised access are relevant.
- Preventive controls are typically more effective than detective controls. For example, preventing a fraud from occurring is far better than simply detecting it after the fact. Therefore, preventive fraud controls are often considered relevant.
- Automated controls are more reliable than manual controls. For example, automated controls that force periodic password changes by users are more reliable than generic policies that have no enforcement. Manual processes are also subject to human error.

Consider IT-based Antifraud Controls
The importance of antifraud controls is something that cannot be overstated, and appropriate attention should be given to this issue. Information technology plays a significant role in the prevention and detection of fraud, as many antifraud controls rely on IT systems. The following examples of IT-based antifraud controls should be considered for inclusion in a company's compliance program:
- Application-enforced segregation of duties—Most systems have the ability to define what privileges are assigned to users within the application. As a result, the system enforces appropriate approvals for transaction processing and prevents users from initiating and authorising their own transactions.
- Access controls—Most systems have privileged users who can access sensitive information, such as payroll data, allowing them to add fictitious employees and thereby commit fraud. Limiting such access to a few people and making sure that the financial reporting personnel do not have this access is important to establishing internal control over financial reporting.

Control Documentation
Documentation may take various forms, including entity policy manuals, IT policies and procedures, narratives, flowcharts, decision tables, procedural write-ups, or completed questionnaires. The extent of documentation may vary, depending upon the size and complexity of the organisation. At the entity level, documentation of IT controls should include an assessment of controls that includes evidence to support the responses and opinions of management. At the activity level, documentation should include a:
- Description of the processes and related subprocesses (may be in narrative form; however, it may be more effective to illustrate as a flowchart)
- Description of the risk associated with the process or subprocess, including an analysis of its impact and probability of occurrence. Consideration should be given to the size and complexity of the process or subprocess and its impact on the organisation's financial reporting process.

- Statement of the control objective designed to reduce the risk of the process or subprocess to an acceptable level
- Description of the control activity(ies) designed and performed to satisfy the control objective related to the process or subprocess. This should include the type of controls (preventive or detective) and the frequency they are performed.
- Description of the approach followed to confirm (test) the existence and operational effectiveness of the control activities
- Conclusions reached about the effectiveness of controls as a result of testing

4. Evaluate Control Design and Operating Effectiveness

This step includes considering the nature of evidence required and the timing of control testing.

Evaluate Control Design
Control design causes an IT organisation to step back and evaluate the ability of its control program to reduce IT risk to an acceptable level. More specifically, it forces management to evaluate the appropriateness of control attributes, including preventive, detective, automated and manual, when concluding on control design. For example, if a change management risk is identified that would result in unauthorised programs being migrated into the production environment, a properly designed control will prevent this from occurring. In this example, a detective control that identifies unauthorised programs in production after the fact may not be appropriate. Control design in the overall IT control environment cannot be overstated.

As discussed earlier, to provide a basis to support management's assertion regarding the adequacy of control design, management needs to document its evaluation of control design. Management's documentation of its evaluation of control design should be sufficiently detailed for the audit team to review the design, perform a walk-through and test the effectiveness of a control. The audit team should be able to understand management's evaluation of control design with sufficient detail to reperform the test of design. Generally, it is not sufficient to provide policies and manuals without providing a reconciliation to the design evaluation process.

Evaluate Operational Effectiveness
Once control design has been assessed, as appropriate, its design and effectiveness should be tested. During this stage, initial and ongoing tests—conducted by individuals responsible for the controls and the internal control programme management team—should be performed to test the design and operating effectiveness of the control activities.

Although there are many factors that go into selecting sample sizes (e.g., other controls being tested, expected error rate), **figure 6** represents a common (minimum) sample selection methodology used by companies and auditors to test the operating effectiveness of controls. For IT general controls, the sample size selected will correspond with the frequency of control operation.

Figure 6—Guidance for Sample Size Selection

Nature of Control	Frequency of Performance	Minimum Sample Size
Manual	Many times per day	25
Manual	Daily	25
Manual	Weekly	5
Manual	Monthly	2
Manual	Quarterly	2
Manual	Annually	1
Automated	Test one application of each programmed control activity (assures IT general controls are effective).	
IT general controls	Follow the guidance above for manual and programmed aspects of IT general controls.	

Management needs to document its tests of operating effectiveness and conclusions on whether the relevant controls evaluated by management are operating as designed. Similar to management's documentation of its evaluation of control design, management needs to document its evaluation of operational effectiveness in sufficient detail for external auditors to reperform the operational effectiveness tests performed by management. In addition to the information documented in the control design evaluation, the documentation of operational effectiveness may include the following information:
- Nature, timing and extent of test steps performed
- Results from testing

- Individual who performed the test and the date performed
- Sample size and test population
- Reference/location of supporting documentation
- Conclusion on operational effectiveness
- Exceptions identified and related remediation plans and/or compensating controls

Consider the Nature of Evidence Required
Different forms of evidence can be obtained in testing the design and operating effectiveness of controls, including inquiries of appropriate personnel, inspection of relevant documentation, observation of the company's operations and reperformance of the application of the control. Forms of evidence include:
- Inquiry—Inquiry is a procedure that consists of seeking information from knowledgeable persons throughout the company. For most organisations, inquiry is used extensively and is often complemented by performing other procedures.
- Inspection of documentation—Because inquiry alone does not provide sufficient evidence to support the design or operating effectiveness of a control, additional tests should be performed. To obtain sufficient evidence about the operating effectiveness of the control, organisations should corroborate inquiries by performing other procedures, such as inspecting reports or other documentation used in performance of the control.
- Observation—In circumstances in which documentary evidence of controls or the performance of controls does not exist and is not expected to exist, organisations should corroborate inquiries of appropriate personnel with observation of company activities.
- Reperformance—In circumstances where the quality of evidence regarding the design or effective operation of controls might not be sufficiently persuasive, organisations may choose to reperform the control and independently run the exception report and investigate exceptions. For example, the signature on an exception report may not be sufficient to demonstrate that all exceptions have been investigated. If this is the case, organisations may chose to reperform the control and independently run the exception report and investigate exceptions.

Consider the Timing of Control Testing
Organisations should perform tests of controls over a period of time that is adequate to determine whether, as of the date specified in management's report, the controls necessary for achieving the objectives of the control criteria are operating effectively. The period of time over which organisations perform tests of controls varies with the nature of the controls being tested and the frequency with which specific controls operate and specific policies are applied. Some controls operate continuously (e.g., approval of user access requests), whilst others operate only at certain times (e.g., periodic review of user access lists). Generally speaking, organisations should perform testing at the time controls are operating.

Roll-forward Testing
For many organisations, testing of IT controls is performed at an interim date (prior to year end). When organisations test controls at an interim date, they should determine what additional evidence to obtain concerning the operation of the control for the remaining period. In making that determination, organisations should consider the:
- Specific controls tested prior to the 'as of' date and the results of those tests
- Degree to which evidence about the operating effectiveness of those controls was obtained
- Length of the remaining period
- Possibility that there have been any significant changes in internal control over financial reporting subsequent to the interim date

5. Prioritise and Remediate Deficiencies

This step includes assessing IT general control deficiencies and considering the aggregate effect.

Identify and Assess IT General Control Deficiencies
All deficiencies, including IT deficiencies, should be reviewed with financial compliance personnel and evaluated as part of the overall internal control certification. IT control deficiencies should not be evaluated in isolation. Similarly, application controls that directly support the financial statement control objectives also need to be reviewed and evaluated with the financial compliance team. Generally speaking, there are two types of deficiencies that companies will have to address:
- Design deficiencies—These are issues related to missing controls, inadequate controls, lack of supporting documentation or other flaws in control design that do not sufficiently mitigate the related risk.
- Operating effectiveness deficiencies—These are issues relating to the consistency with which controls are operating, such as not performing a control as designed consistently throughout the year.

Consider the Aggregate Effect of Deficiencies
In some cases, individual control deficiencies may be considered insignificant, yet when combined with other similar deficiencies, the effect may be more significant. For example, an organisation that does not perform a periodic review of user access lists to its financial application would normally be considered to have a control design deficiency. On its own, it may not be significant, especially if other compensating controls exist. However, if this organisation also failed to properly authorise user access requests for the same application, the aggregate effect of the two deficiencies may result in a significant deficiency or material weakness. In other words, the combined effect of control deficiencies related to user access requests and user access reviews could place into question the validity of users' access within the financial application and, therefore, place into question the validity of transactions within the system as well.

Remediate Control Deficiencies
The remediation phase of most projects is where significant effort and money is spent. In some cases, there may be short-term options for remediation that may not be expensive to implement and can be implemented quickly, but may cost more to operate. For instance, the manual process for adding, changing and deleting users in systems is time-consuming and slow. However, a longer-term solution might include process automation that restricts user access provisioning without appropriate authorisation. This approach will definitely cost more in the near term, but tends to be far more reliable and cost-effective in the long term.

6. Build Sustainability

At this point, IT management should be in a position to assess the IT internal control program effectiveness. Effective internal controls, control assessment and management competencies should become part of the IT department's organisation and culture and sustain themselves over the long term. Control is not an event; it is a process that requires continuous support and evaluation to stay current. The ultimate objective is to convert the IT control project into a process. The following activities should be considered to achieve this:
- Performing a post-implementation review, identifying what went right and areas for improvement
- Reviewing other independent material for suggestions and opportunities to improve the approach
- Meeting with peers in other organisations to discuss potential improvements to the process
- Assessing longer-term solutions, such as automation of processes and implementation of program change control software
- Developing a preliminary plan and timetable for the following year, making it an ingrained process

Rationalise Controls
Control rationalisation (or elimination) is another initiative that should take place in the sustainment phase. Undoubtedly, there will be some controls that are documented that, over time, become less and less useful. Companies should periodically review their controls to identify which controls can be eliminated from the control listing. In doing so, consideration should be given to the impact of removing a control and any documentation prepared—explaining why the control was removed.

Automate Controls
In most cases, there is a significant number of manual controls that can be automated. Companies can review manual controls to determine which can be transformed into automated controls. In many cases, more detailed information will be needed, depending on the applications available to a company and the nature of controls that are desired. Some organisations have more detailed control benchmarks that provide such details for a given application, such as SAP and Oracle.

Perform Application Benchmarking
The concept of application benchmarking is that, once an application is shown to be reliable through testing, it may not have to be tested every year. As a result, reductions in effort can be realised, making the compliance process more efficient and effective.

CONCLUSION

There is no such thing as a risk-free environment, and an effective program of IT controls does not create such an environment. However, the process that most organisations will follow to enhance their system of internal control over financial reporting is likely to provide lasting benefits. Good IT governance over planning and life cycle control objectives should result in more accurate and timely financial reporting. The work required to audit IT controls over financial reporting should be regarded as an opportunity to establish strong governance models designed to result in accountability and responsiveness to business requirements.

APPENDIX—COBIT COMPONENTS FOR FIVE IT PROCESSES

COBIT's good practices are strongly focused on controls that will help ensure effective service delivery. To achieve effective governance, executives expect controls to be implemented by operational managers within a defined control framework for all IT processes. COBIT's IT control objectives are organised by IT process to provide a clear link among IT governance requirements and IT controls. The complete *COBIT 4.1* publication is posted for download on *www.isaca.org/cobit*.

COBIT FRAMEWORK NAVIGATION

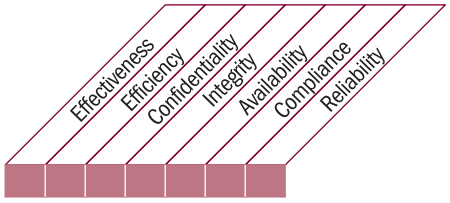
The COBIT framework defines 34 IT processes divided into four IT domains: Plan and Organise (PO), Acquire and Implement (AI), Deliver and Support (DS), and Monitor and Evaluate (ME). For each of the 34 IT processes, COBIT provides control objectives and management guidelines, control practices and IT assurance guidelines.

Each IT process section presents control statements, business requirements, enablers and considerations. The domain indicator (PO, AI, DS and ME) is shown at top left in this IT process section. The applicable information criteria and IT resources managed are shown in **figure 7**.

DS2 is used as an example and the components for eight additional COBIT processes follow.

Figure 7—COBIT Navigation

Within each IT process, control objectives are provided as generic action statements of the minimum management good practices to ensure that the process is kept under control.



Control over the IT process of

process name

that satisfies the business requirement for IT of

summary of most important IT goals

by focusing on

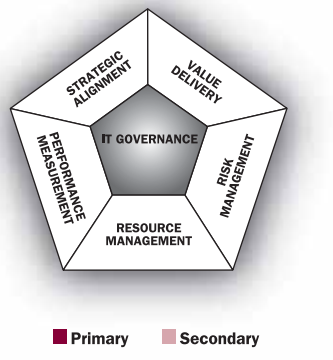
summary of most important process goals

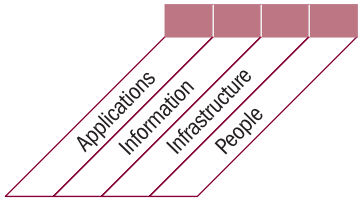
is achieved by

activity goals

and is measured by

key metrics





DS2 COBIT COMPONENTS WITH ADDITIONAL GUIDANCE

The navigational outline of the COBIT framework shows how to navigate through the COBIT product set. All of the COBIT components of the COBIT process DS2 *Manage third-party services* are explained and linked to each other.

Concept and Importance of DS2

Many entities now use outsourcing for support services within their IT function all the way through to complete outsourcing of all their IT functions to a third party. An entity might contract the repair and maintenance of its personal computers to a third party, place its internal and external networks in the hands of a telecommunications specialist, or employ web-based software from an application service provider, such as NetSuite, that provides customer relationship management (CRM) and ERP functionality across the Internet. Whenever an entity employs outsourcing, it takes advantage of the benefits of scale of operations and specialist expertise of the provider. The entity can concentrate on what it does best—be it running public services in a municipality or developing and manufacturing high-performance sports equipment. Of course, outsourcing of IT services means that the entity is now dependent on the outsourcing vendor to manage operations that are likely critical to its business model. Imagine a firm that cannot access the Internet or whose e-commerce servers are no longer available to the public or its business partners. So, management of third-party services is an important task for IT and operational management in entities that outsource services to third parties.

An Example of Strategic Outsourcing
CIO magazine reported on the outsourcing by Merrill Lynch, a large retail securities broker and financial services advisor in the US, of a major element of its core information technology. Thomson Financial Services now acts as the primary contractor in developing and maintaining Merrill Lynch's 'wealth management workstation platform', which is used by its 14,000 financial advisors in assisting their clients. Thomson, in turn, subcontracts to companies such as AT&T, Cap Gemini Ernst & Young, Dell, HP, IBM and Microsoft. Merrill Lynch's contract with Thomson includes 'service level agreements (SLAs), sets out performance bonuses, establishes penalties and covers more than a few other details'.

Source: *CIO* Magazine, September 2003 (*www.cio.com/archive/091503/billion.html*)

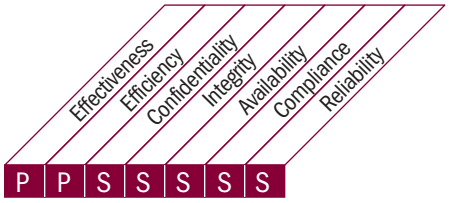
DS2 IT Process

The IT process for DS2 *Manage third-party services* does not necessarily satisfy the different business requirements for information (effectiveness, efficiency, confidentiality, integrity, availability, compliance, reliability) to the same degree. Therefore, the degree to which the process impacts the information criterion concerned is indicated as primary (P) or secondary (S). It also provides an overview of the IT resources that are specifically managed by the process under review.

PROCESS DESCRIPTION

DS2 Manage Third-party Services

The need to assure that services provided by third parties (suppliers, vendors and partners) meet business requirements requires an effective third-party management process. This process is accomplished by clearly defining the roles, responsibilities and expectations in third-party agreements as well as reviewing and monitoring such agreements for effectiveness and compliance. Effective management of third-party services minimises the business risk associated with non-performing suppliers.



Control over the IT process of

Manage third-party services

that satisfies the business requirement for IT of

providing satisfactory third-party services whilst being transparent about benefits, costs and risks

by focusing on

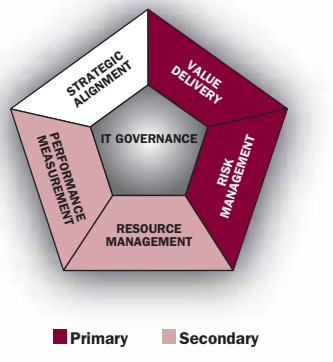
establishing relationships and bilateral responsibilities with qualified third-party service providers and monitoring the service delivery to verify and ensure adherence to agreements

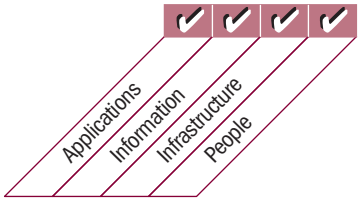
is achieved by

- Identifying and categorising supplier services
- Identifying and mitigating supplier risk
- Monitoring and measuring supplier performance

and is measured by

- Number of user complaints due to contracted services
- Percent of major suppliers meeting clearly defined requirements and service levels
- Percent of major suppliers subject to monitoring





DS2 Control Objectives

The control objectives emphasise the importance of documented supplier interfaces and ownership for managing the quality of relations with third parties. Third-party contracts and outsourcing contracts should be clearly defined and mutually agreed upon, and, before selection, the potential third parties should go through a quality check to make sure that they can deliver the required services. Agreements should be made regarding continuity of services and security issues. Finally, a monitoring process should be established to ensure that the services are delivered as agreed.

The control objectives can be used proactively by corporations to manage their third-party relationships. For example, as an entity negotiates its IT outsourcing agreements, it can use DS2 as a guide for planning the strategic and contractual relationships between the entity and the outsourcing partner(s). Of course, the systems that are put in place at the commencement of an outsourcing arrangement may not be maintained. They may no longer match changing business dynamics as the activities of the contracting entity respond to changing markets. An auditor can employ DS2 as a foundation for determining the extent of audit effort in assessing the quality of internal controls over the outsourcing agreement.

DS2.1 Identification of All Supplier Relationships
Identify all supplier services, and categorise them according to supplier type, significance and criticality. Maintain formal documentation of technical and organisational relationships covering the roles and responsibilities, goals, expected deliverables, and credentials of representatives of these suppliers.

DS2.2 Supplier Relationship Management
Formalise the supplier relationship management process for each supplier. The relationship owners should liaise on customer and supplier issues, and ensure the quality of the relationship based on trust and transparency (e.g., through SLAs).

DS2.3 Supplier Risk Management
Identify and mitigate risks relating to suppliers' ability to continue effective service delivery in a secure and efficient manner on a continual basis. Ensure that contracts conform to universal business standards in accordance with legal and regulatory requirements. Risk management should further consider non-disclosure agreements (NDAs), escrow contracts, continued supplier viability, conformance with security requirements, alternative suppliers, penalties and rewards, etc.

DS2.4 Supplier Performance Monitoring
Establish a process to monitor service delivery to ensure that the supplier is meeting current business requirements and continuing to adhere to the contract agreements and SLAs, and that performance is competitive with alternative suppliers and market conditions.

DS2 Management Guidelines

COBIT was initially created from a control and audit perspective, which explains why the control objectives and audit guidelines were the first major components of the COBIT framework. However, ITGI identified the growing need of management for measurability of IT. To respond to this need, in 2000 ITGI developed the COBIT management guidelines with tools to assess and measure the organisation's IT environment in the 34 IT processes. These management guidelines included maturity models (MMs), critical success factors (CSFs), KGIs and KPIs for each process.

In *COBIT 4.1*, the management guidelines are included and the terms KGI and KPI have been replaced with two types of metrics:
- Outcome measures, previously KGIs, indicate whether the goals have been met. These can be measured only after the fact and, therefore, are called 'lag indicators'.
- Performance indicators, previously KPIs, indicate whether goals are likely to be met. They can be measured before the outcome is clear and, therefore, are called 'lead indicators'.

In *COBIT 4.1*, CSFs have been transformed into value drivers and risk drivers provided in the *COBIT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition* and *IT Assurance Guide: Using COBIT®*.

MANAGEMENT GUIDELINES

DS2 Manage Third-party Services

From	Inputs
PO1	IT sourcing strategy
PO8	Acquisition standards
AI5	Contractual arrangements, third-party relationship management requirements
DS1	SLAs, contract review report
DS4	Disaster service requirements, including roles and responsibilities

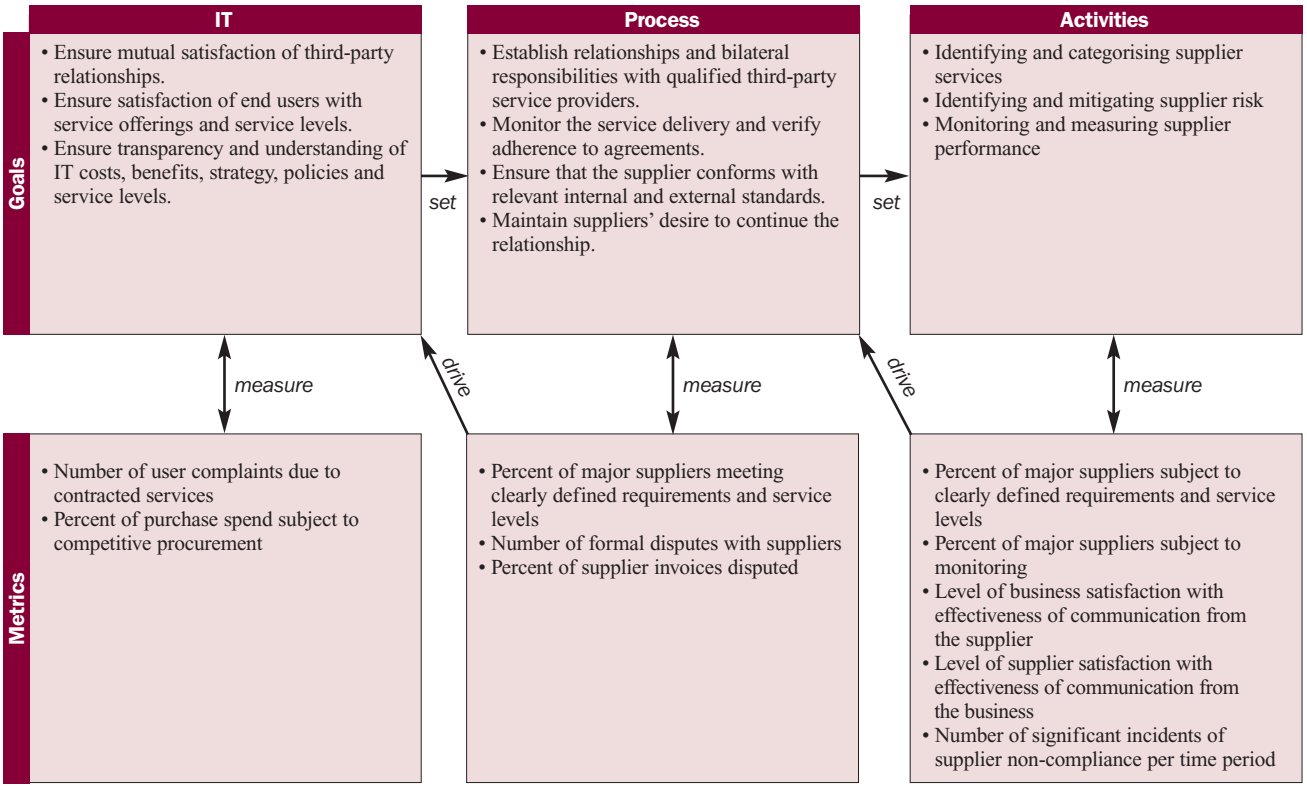
Outputs	To
Process performance reports	ME1
Supplier catalogue	AI5
Supplier risks	PO9

RACI Chart

Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Identify and categorise third-party service relationships.				I	C	R	C	R	A/R	C	C
Define and document supplier management processes.		C		A	I	R	I	R	R	C	C
Establish supplier evaluation and selection policies and procedures.		C		A	C	C		C	R	C	C
Identify, assess and mitigate supplier risks.		I		A		R		R	R	C	C
Monitor supplier service delivery.				R	A	R		R	R	C	C
Evaluate long-term goals of the service relationship for all stakeholders.	C	C	C	A/R	C	C	C	C	R	C	C

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



A maturity model is a method of scoring that enables the organisation to grade its maturity for a certain process from nonexistent (0) to optimised (5). This tool offers an easy-to-understand way to determine the 'as is' and the 'to be' (according to enterprise strategy) positions, and enables the organisation to benchmark itself against best practices and standard guidelines. In this way, gaps can be identified and specific actions can be defined to move toward a desired position (to be). When doing this maturity assessment, it is important to comply with the basic principles of maturity measurement: one can move to a higher maturity only when all conditions described in a certain maturity level are fulfilled.

The maturity model for DS2 *Manage third-party services*, which is shown in the following section, declares that an organisation is at maturity level 1 for this process when management is aware of the need to have documented policies and procedures for third-party service procurement and signed contracts, but the measurement of the service is informal and reactive. An organisation achieves, for example, maturity level 4 when responsibilities for contract and vendor management are assigned and when formal and standardised criteria are provided for defining scope of work, services to be provided, deliverables, etc.

The maturity model is a very useful scanning mechanism for a variety of participants in the IT governance process. When reporting to the audit committee of the board, IT management can provide a highly useful categorisation of the sophistication of controls in place for each of the processes encompassed by COBIT. For example, assume that an entity has a number of major IT outsourcing agreements that are fundamental to meeting the entity's operational objectives. If IT management or a consultant reports to the audit committee that the maturity model relating to the controls implicit in DS2 is at, say, level 2, the audit committee would likely be concerned and seek immediate improvements. Conversely, if the maturity is assessed at level 4, the audit committee would seek further improvements but in a staged and measured fashion.

DS2 Maturity Model

Management of the process of *Manage third-party services* that satisfies the business requirement for IT of *providing satisfactory third-party services whilst being transparent about benefits, costs and risks* is:

0 **Non-existent** when
responsibilities and accountabilities are not defined. There are no formal policies and procedures regarding contracting with third parties. Third-party services are neither approved nor reviewed by management. There are no measurement activities and no reporting by third parties. In the absence of a contractual obligation for reporting, senior management is not aware of the quality of the service delivered.

1 **Initial/*Ad Hoc*** when
management is aware of the need to have documented policies and procedures for third-party management, including signed contracts. There are no standard terms of agreement with service providers. Measurement of the services provided is informal and reactive. Practices are dependent on the experience (e.g., on demand) of the individual and the supplier.

2 **Repeatable but Intuitive** when
the process for overseeing third-party service providers, associated risks and the delivery of services is informal. A signed, pro forma contract is used with standard vendor terms and conditions (e.g., the description of services to be provided). Reports on the services provided are available, but do not support business objectives.

3 **Defined** when
well-documented procedures are in place to govern third-party services, with clear processes for vetting and negotiating with vendors. When an agreement for the provision of services is made, the relationship with the third party is purely a contractual one. The nature of the services to be provided is detailed in the contract and includes legal, operational and control requirements. The responsibility for oversight of third-party services is assigned. Contractual terms are based on standardised templates. The business risk associated with the third-party services is assessed and reported.

4 **Managed and Measurable** when
formal and standardised criteria are established for defining the terms of engagement, including scope of work, services/deliverables to be provided, assumptions, schedule, costs, billing arrangements and responsibilities. Responsibilities for contract and vendor management are assigned. Vendor qualifications, risks and capabilities are verified on a continual basis. Service requirements are defined and linked to business objectives. A process exists to review service performance against contractual terms, providing input to assess current and future third-party services. Transfer pricing models are used in the procurement process. All parties involved are aware of service, cost and milestone expectations. Agreed-upon goals and metrics for the oversight of service providers exist.

5 **Optimised** when
contracts signed with third parties are reviewed periodically at predefined intervals. The responsibility for managing suppliers and the quality of the services provided is assigned. Evidence of contract compliance to operational, legal and control provisions is monitored, and corrective action is enforced. The third party is subject to independent periodic review, and feedback on performance is provided and used to improve service delivery. Measurements vary in response to changing business conditions. Measures support early detection of potential problems with third-party services. Comprehensive, defined reporting of service level achievement is linked to the third-party compensation. Management adjusts the process of third-party service acquisition and monitoring based on the measurers.

DS2 Control Practices

Control practices expand the capabilities of COBIT by providing the practitioner with an additional level of detail. The current COBIT IT processes, business requirements and control objectives define *what* needs to be done to implement an effective control structure. The control practices provide the more detailed *why* and *how* needed by management, service providers, end users and control professionals to implement highly specific controls based on an analysis of operational and IT risks.

Managing third-party services is important to facilitate effective and efficient communication between organisations to help maintain effective service delivery. This can be achieved by implementing control practices, such as having a policy and procedure to maintain a register of key suppliers and ensuring that this register is continuously updated via a regular review process.

DS2.1 Identification of All Supplier Relationships
Value drivers:
- Centralised service supplier overview to support supplier decision making
- Preferred suppliers identified for future acquisitions
- Supplier management resources focused on critical suppliers

Risk drivers:
- Unidentified significant and critical suppliers
- Inefficient and ineffective usage of supplier management resources
- Unclear roles and responsibilities leading to miscommunications, poor services and increased costs

Control practices
1. Define and regularly review criteria to identify and categorise all supplier relationships according to the supplier type, significance and criticality of service. The list should include a category describing vendors as preferred, non-preferred or not recommended.
2. Establish and maintain a detailed register of suppliers, including name, scope, purpose of the service, expected deliverables, service objectives and key contact details.

DS2.2 Supplier Relationship Management
Value drivers:
- Relationships promoted that support the overall enterprise objectives (both business and IT)
- Effective and efficient communication and problem resolution
- Clear ownership of responsibilities between customer and supplier

Risk drivers:
- Supplier not responsive or committed to the relationship
- Problems raised and issues not resolved
- Inadequate service quality

Control practices:
1. Define and formalise roles and responsibilities for each service supplier.
2. Assign relationship owners for all suppliers and make them accountable for the quality of service(s) provided.
3. Document the supplier relationship managers and communicate the information within the organisation.
4. Establish and document a formal communication process between the organisation and the service provider.
5. Ensure that contracts with key service suppliers provide for a review of supplier internal controls by management or independent third parties.

6. Regularly review the reports between the organisation and the service supplier.
7. Register incidents caused by suppliers and report them using the company's internal incident management process.
8. Periodically review and assess supplier performance against established and agreed-upon service levels. Clearly communicate suggested changes to the service supplier.

DS2.3 Supplier Risk Management
Value drivers:
• Compliance with legal and contractual requirements
• Reduced incidents and potential losses
• Identification of low-risk, well-managed suppliers

Risk drivers:
• Non-compliance with regulatory and legal obligations
• Security as well as other incidents
• Financial losses and reputational damage because of service interruption

Control practices:
1. Identify and monitor supplier risks in accordance with the organisation's established risk management process.
2. Identify and document in the contract supplier risks (and remedies) associated with the supplier's inability to fulfil the contractual agreement(s).
3. When defining the contract, consider remedies including software escrow agreements, alternative suppliers or standby agreements in the event of supplier failure.
4. Review all contracts for legal and regulatory requirements.

DS2.4 Supplier Performance Monitoring
Value drivers:
• Timely detection of service level non-compliance
• Benefits of service contracts realised
• Costs controlled
• Costly disputes and possible litigation avoided

Risk drivers:
• Undetected service degradation
• Inability to challenge costs and service quality
• Inability to optimise choice of suppliers

Control practices:
1. Define and document criteria to monitor service suppliers' performance.
2. Ensure that the supplier regularly reports on agreed-upon performance criteria.
3. Invite users to provide feedback for assessment of supplier performance and quality of service.
4. Evaluate the costs and market conditions for the service levels by benchmarking against alternative suppliers, and identify potential for improvement.
5. Define arbitration procedures to consult an arbitration committee before bringing an action.

Example of IT Outsourcing Risks—Loss of Important Information
Dr. Larry Ponemon reports on a case study of a US-based corporation that outsourced major IT operational functions to the Ukraine. This location was chosen because:

- The workforce was well educated and the vendor had the necessary call center setup skills
- The cost of operations was very favorable and included significant tax incentives provided by the government
- The outsourcing industry in the Ukraine was booming

Ponemon reports that:

> *After the decision was made, the company's legal and procurement team formulated contracts with the vendor to ensure that it took full responsibility for complying with the privacy policy, which included a strict do-not-share with third parties for secondary uses without consent, and all US regulatory requirements. The Ukraine vendor also agreed by legal contract to comply with strict data protection and information security requirements as suggested by the US Federal Trade Commission's Safeguards Rule.*

Unfortunately, after a relatively short period, the company experienced many problems with billing, identity theft and fraud on customer bank accounts. According to Ponemon, a forensic expert found that the source of the information leak was in the Ukraine and undertaken by a new IT employee. Ponemon notes that:

> *While the IT employee did not have a criminal history, her husband was a convicted mobster on a US cybercrime watch list. She claimed that her company did not explain security and privacy requirements to employees. She believed that the downloading and sharing of information would not harm anyone.*

Source: *CIO* magazine, April 2004

DS2 IT Assurance Guidelines

In addition to and corresponding with each of the 34 IT processes, COBIT provides audit guidelines. The goal of these guidelines is to enable the review of IT processes against the recommended detailed control objectives. This can help the IT auditor to:
- Provide management with reasonable assurance that the control objectives are being met
- Substantiate the resulting risks, where there are significant control weaknesses
- Advise management on corrective actions

COBIT applies a generally accepted structure for performing this audit process:
1. Obtaining an understanding of business requirements, related risks and relevant control measures within the process that will be audited. A thorough understanding of the activities underlying the control objectives and the stated control measures and procedures is an essential first step in the audit process.
2. Evaluating the appropriateness of stated controls in the IT process. The appropriateness can be evaluated by considering identified criteria and industry best practices, reviewing critical success factors of the control measures and applying professional judgement of the auditor.
3. Assessing compliance by testing whether the stated controls are working as prescribed, consistently and continuously
4. Substantiating the risk of control objectives not being met by using analytical techniques and/or consulting alternative sources. The goal is to make clear the nature of the risks by, for example, shocking management into action.

The DS2 *Manage third-party services* audit process illustrated in the following test the control design section is typically used by an auditor to design a detailed audit programme. Obtaining an understanding of the process (policies, procedures, responsibilities, etc.) can, for example, be achieved by interviewing the CIO, IT senior management, etc. The controls and procedures can be evaluated, for example, by checking their consistency with the general organisational policies. Compliance can be assessed by examining whether the controls are followed as prescribed and, for example, testing whether contracts contain all the prescribed elements. Finally, the risk of control objectives not being met could be substantiated by benchmarking third-party services against similar organisations or international standards.

Test the Control Design
DS2.1 *Identification of all supplier relationships:*
- Enquire whether and confirm that a register of supplier relationships is maintained.

- Obtain and inspect supplier relationship criteria for reasonableness and completeness of categorisations by supplier type, significance and criticality.
- Determine if the supplier categorisation scheme is sufficiently detailed to categorise all supplier relationships based on the nature of contracted services.
- Verify whether past histories on supplier selection/rejection are kept and used.
- Inspect the register of supplier relationships to ensure that it is up to date, appropriately categorised and sufficiently detailed to ensure that it provides a foundation for monitoring of existing suppliers.
- Inspect a representative sample of supplier contracts, SLAs and other documentation to ensure that they correspond with the supplier register.

DS2.2 *Supplier relationship management*:
- Inspect service supplier documentation for evidence of formalised roles and responsibilities, and determine if supplier management roles have been documented and communicated within the organisation.
- Determine if policies exist to address the need for formal contracts, definition of content of contracts, and assignment of owner or relationship manager responsibilities for ensuring that contracts are created, maintained, monitored and renegotiated as required.
- Assess if the assignment of supplier management roles is reasonable and based on the level and technical skills required to effectively manage the relationship.

DS2.3 *Supplier risk management:*
- Enquire whether risks associated with the inability to fulfil the supplier contracts are defined.
- Enquire whether remedies were considered when defining the supplier contract.
- Inspect contract documentation for evidence of review.
- Enquire of key staff members whether a risk management process exists to identify and monitor supplier risk.
- Determine if policies exist requiring independence within the vendor sourcing and selection process, and between vendor and management personnel within the organisation.

DS2.4 *Supplier performance monitoring:*
- Select a sample of supplier invoices, determine if they identify charges for contracted services, as specified within service contracts, and assess the reasonableness of charges compared to various internal, external and industry comparable performance.
- Inspect a sample of supplier service reports to determine if the supplier regularly reports on agreed-upon performance criteria and if performance reporting is objective and measurable and in alignment with defined SLAs and the supplier contract.

DS2 Test the Outcome of the Control Objectives
- For a sample of suppliers, assess if supplier records are aligned to the defined catogorisation scheme used to identify and categorise all supplier relationships.
- Obtain and validate the list of supplier relationship criteria for completeness, and review suppliers' records against the catogorisation scheme used to identify and categorise all supplier relationships. Assess if supplier type, significance and criticality of services provided have been documented.
- Obtain a register of suppliers, and verify the accuracy of data through inspection of a sample of service contracts.
- Obtain a register of suppliers, and verify the accuracy of data. Consideration should be given to organisational changes or recent changes in the IT landscape that would require changes in the supplier relationship criteria.
- Determine if supplier documentation is sufficiently detailed to identify methods of communication, prioritisation of services and escalation procedures, minimum service levels, and operational objectives.
- Ascertain if documentation clearly delineates responsibilities between the service provider and the user organisation.
- Determine if service supplier documentation is centrally managed and maintained and if a process exists for the periodic review and updating of documents.
- Perform a detailed review of each third-party contract to determine the existence of qualitative and quantitative provisions confirming obligations, including provisions for co-ordinating and communicating the relationship between the provider and user of information services.
- Determine if policies exist for management's periodic review of service supplier reporting, and select a sample of supplier reports for evidence of management's review.
- Obtain and inspect service supplier incident reports for existence, and determine if incidents were categorised and escalated according to agreed-upon levels of severity and if they were tracked and communicated within the organisation until resolved. Reported incidents should include communication to supplier management and users of the services.
- Verify that goals and expected service levels are periodically reviewed to ensure that they continue to support current business requirements, and that suggested changes are communicated clearly to service suppliers.

- Inspect the supplier register for assignment of a relationship manager, and obtain and inspect evidence of a service supplier communication process.
- Obtain and review contracts for existence of clauses relating to third-party reviews, and determine if management has obtained and reviewed reports from such reviews.
- For a sample of suppliers, inspect available documentation to determine if supplier risk has been considered and if identified risk has been addressed/mitigated.
- For a sample of supplier relationships, determine if the following have been addressed within the supplier contract:
  – Security requirements
  – Non-disclosure guarantees
  – Right to access and right to audit
  – Formal management and legal approval
  – Legal entity providing services
  – Services provided
  – SLAs, both qualitative and quantitative
  – Cost of services and frequency of payment for services
  – Resolution of problem process
  – Penalties for non-performance
  – Dissolution process
  – Modification process
  – Reporting of service—content, frequency and distribution
  – Roles between contracting parties during the life of the contract
  – Continuity assurances that services will be provided by the vendor
  – Communications process and frequency between the user of services and provider
  – Duration of contract
  – Level of access provided to vendor
  – Regulatory requirements

DS2 Document the Impact of the Control Weaknesses

- Through inquiry of user and IT management and benchmarking of the organisation to similarly sized organisations and organisations within the same industry, identify any supplier relationships that have been excluded from the supplier register. Consider the following supplier relationships:
  – Private branch exchange (PBX) suppliers
  – Paper and form suppliers
  – Maintenance support suppliers
  – Offsite data storage and hot-site services providers
  – Service organisations providing data processing (e.g., ASP, co-location)
  – External software developers and quality assurance
- Enquire of supplier management to ascertain if they are knowledgeable of the nature of the service supplier relationship and contracted services.
- Inspect a sample of service supplier billings for out-of-scope billings, and determine the involvement of supplier management in reviewing and approving the overage.
- For a sample of service suppliers, obtain the supplier's reported performance metrics, and review for deviations from agreed-upon performance objectives. Determine if supplier management was aware of any deviations and the reasonableness of actions taken for deviation (e.g., establishment of action plan, service fee penalties for non-performance).
- For a sample of supplier relationships, determine if the level of services compares to the stated contractual obligations. For changes in the supplier relationships, determine if the risk assessments have been updated and if the supplier contract has been appropriately modified.
- Inspect a sample of supplier-reported performance metrics, and identify where performance objectives have not consistently been attained.
- Determine if management has identified and assessed the performance failures, and if an assessment has been performed, re-evaluate the relationship or evaluate the need for modifying the relationship.
- For supplier relationships with the greatest impact on the organisation, determine if contingency plans exist for the recovery or secondary sourcing of contracted services.
- Determine the availability of supplier third-party assessments (e.g., SAS No. 70, ISA 402 or attestation reports) or audit reports and whether management has received and reviewed the reports. For reported control deficiencies (i.e., report qualifications, testing exceptions), determine if management has discussed the deficiencies with the supplier and if an action plan has been implemented. Through review of past or subsequent reports, determine if the supplier promptly remediates control deficiencies.

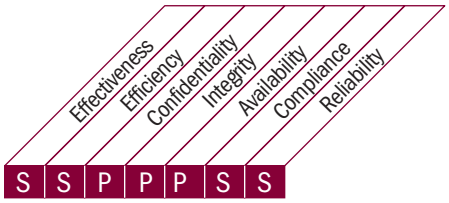
- Determine if key suppliers are included in the annual risk assessment and audit planning process.
- Inspect a sample of supplier-reported performance metrics, and identify where performance objectives have not consistently been attained.
- Determine if management has identified and assessed the performance failures, and if corrective action and a process for ongoing monitoring has been implemented.
- For a sample of service suppliers, obtain the supplier's reported performance metrics, and review them for deviations from agreed-upon performance objectives.
- Determine if supplier management is aware of the deviation and the reasonableness of actions taken (e.g., establishment of action plan, service fee penalties for non-performance).

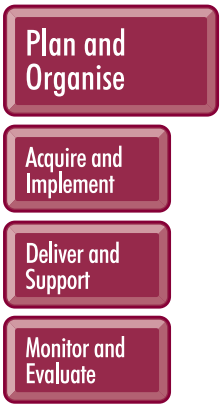
P09 COBIT COMPONENTS

PROCESS DESCRIPTION

P09 Assess and Manage IT Risks

A risk management framework is created and maintained. The framework documents a common and agreed-upon level of IT risks, mitigation strategies and residual risks. Any potential impact on the goals of the organisation caused by an unplanned event is identified, analysed and assessed. Risk mitigation strategies are adopted to minimise residual risk to an accepted level. The result of the assessment is understandable to the stakeholders and expressed in financial terms, to enable stakeholders to align risk to an acceptable level of tolerance.





Control over the IT process of

Assess and manage IT risks

that satisfies the business requirement for IT of

analysing and communicating IT risks and their potential impact on business processes and goals

by focusing on

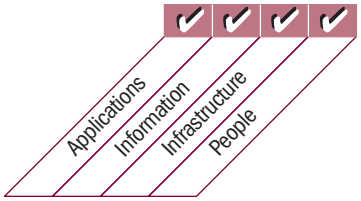
development of a risk management framework that is integrated in business and operational risk management frameworks, risk assessment, risk mitigation and communication of residual risk

is achieved by

- Ensuring that risk management is fully embedded in management processes, internally and externally, and consistently applied
- Performing risk assessments
- Recommending and communicating risk remediation action plans

and is measured by

- Percent of critical IT objectives covered by risk assessment
- Percent of identified critical IT risks with action plans developed
- Percent of risk management action plans approved for implementation



PO9 Control Objectives

PO9.1 IT Risk Management Framework
Establish an IT risk management framework that is aligned to the organisation's (enterprise's) risk management framework.

PO9.2 Establishment of Risk Context
Establish the context in which the risk assessment framework is applied to ensure appropriate outcomes. This should include determining the internal and external context of each risk assessment, the goal of the assessment, and the criteria against which risks are evaluated.

PO9.3 Event Identification
Identify events (an important realistic threat that exploits a significant applicable vulnerability) with a potential negative impact on the goals or operations of the enterprise, including business, regulatory, legal, technology, trading partner, human resources and operational aspects. Determine the nature of the impact and maintain this information. Record and maintain relevant risks in a risk registry.

PO9.4 Risk Assessment
Assess on a recurrent basis the likelihood and impact of all identified risks, using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk should be determined individually, by category and on a portfolio basis.

PO9.5 Risk Response
Develop and maintain a risk response process designed to ensure that cost-effective controls mitigate exposure to risks on a continuing basis. The risk response process should identify risk strategies such as avoidance, reduction, sharing or acceptance; determine associated responsibilities; and consider risk tolerance levels.

PO9.6 Maintenance and Monitoring of a Risk Action Plan
Prioritise and plan the control activities at all levels to implement the risk responses identified as necessary, including identification of costs, benefits and responsibility for execution. Obtain approval for recommended actions and acceptance of any residual risks, and ensure that committed actions are owned by the affected process owner(s). Monitor execution of the plans, and report on any deviations to senior management.

MANAGEMENT GUIDELINES

PO9 Assess and Manage IT Risks

From	Inputs
PO1	Strategic and tactical IT plans, IT service portfolio
PO10	Project risk management plan
DS2	Supplier risks
DS4	Contingency test results
DS5	Security threats and vulnerabilities
ME1	Historical risk trends and events
ME4	Enterprise appetite for IT risks

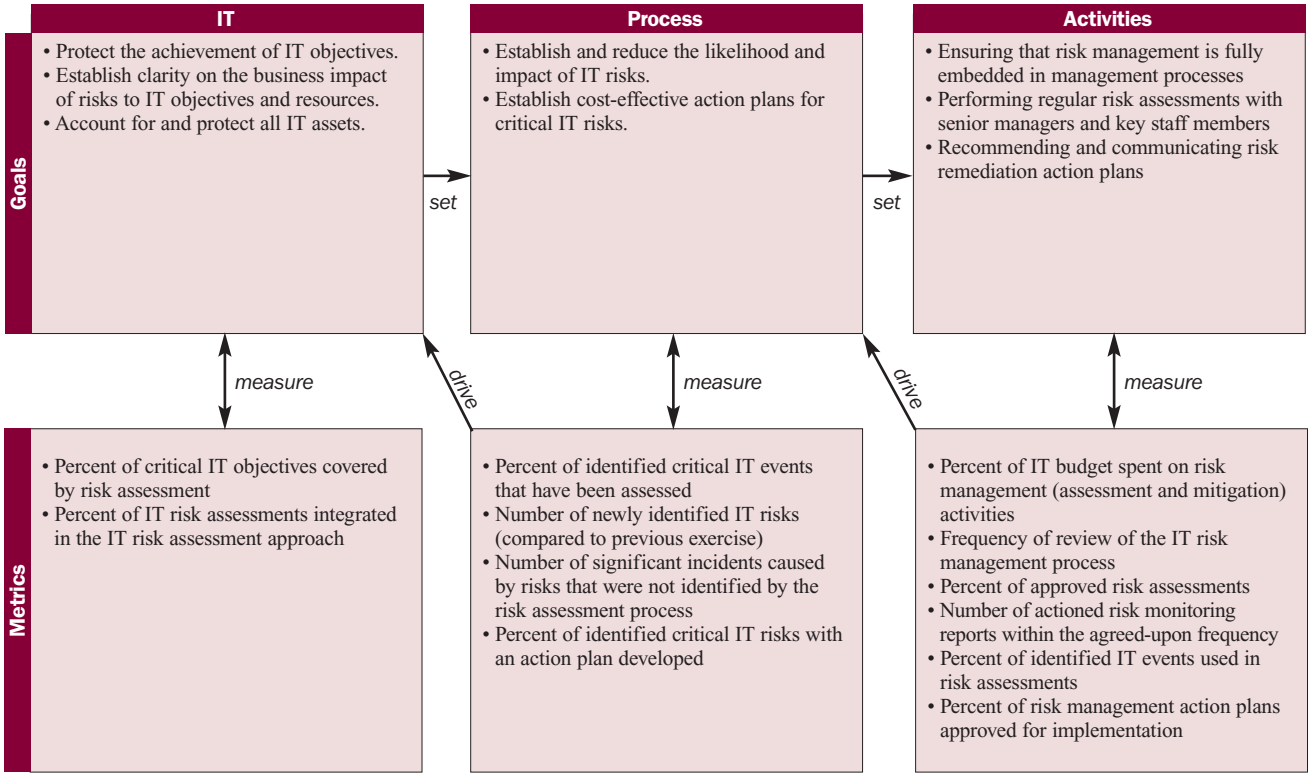
Outputs	To						
Risk assessment	PO1	DS4	DS5	DS12	ME4		
Risk reporting	ME4						
IT-related risk management guidelines	PO6						
IT-related risk remedial action plans	PO4	AI6					

RACI Chart

Activities / Functions	CEO	CFO	Business Executive	CIO	Business Senior Mangement	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Determine risk management alignment (e.g., assess risk).	A	R/A	C	C	R/A	I					I
Understand relevant strategic business objectives.		C	C	R/A	C	C					I
Understand relevant business process objectives.				C	C	R/A					I
Identify internal IT objectives, and establish risk context.					R/A		C	C	C		I
Identify events associated with objectives (some events are business-oriented [business is A]; some are IT-oriented [IT is A, business is C]).	I			A/C	A	R	R	R	R		C
Assess risk associated with events.				A/C	A	R	R	R	R		C
Evaluate and select risk responses.	I	I	A	A/C	A	R	R	R	R		C
Prioritise and plan control activities.	C	C	A	A	R	R	C	C	C		C
Approve and ensure funding for risk action plans.		A	A		R	I	I	I	I		I
Maintain and monitor a risk action plan.	A	C	I	R	R	C	C	C	C	C	R

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



PO9 Maturity Model

Management of the process of *Assess and manage IT risks* that satisfies the business requirement for IT of *analysing and communicating IT risks and their potential impact on business processes and goals* is:

0 **Non-existent** when
risk assessment for processes and business decisions does not occur. The organisation does not consider the business impacts associated with security vulnerabilities and development project uncertainties. Risk management is not identified as relevant to acquiring IT solutions and delivering IT services.

1 **Initial/*Ad Hoc*** when
IT risks are considered in an *ad hoc* manner. Informal assessments of project risk take place as determined by each project. Risk assessments are sometimes identified in a project plan but are rarely assigned to specific managers. Specific IT-related risks, such as security, availability and integrity, are occasionally considered on a project-by-project basis. IT-related risks affecting day-to-day operations are seldom discussed at management meetings. Where risks have been considered, mitigation is inconsistent. There is an emerging understanding that IT risks are important and need to be considered.

2 **Repeatable but Intuitive** when
a developing risk assessment approach exists and is implemented at the discretion of the project managers. The risk management is usually at a high level and is typically applied only to major projects or in response to problems. Risk mitigation processes are starting to be implemented where risks are identified.

3 **Defined** when
an organisationwide risk management policy defines when and how to conduct risk assessments. Risk management follows a defined process that is documented. Risk management training is available to all staff members. Decisions to follow the risk management process and receive training are left to the individual's discretion. The methodology for the assessment of risk is convincing and sound, and ensures that key risks to the business are identified. A process to mitigate key risks is usually instituted once the risks are identified. Job descriptions consider risk management responsibilities.

4 **Managed and Measurable** when
the assessment and management of risk are standard procedures. Exceptions to the risk management process are reported to IT management. IT risk management is a senior management-level responsibility. Risk is assessed and mitigated at the individual project level and also regularly with regard to the overall IT operation. Management is advised on changes in the business and IT environment that could significantly affect the IT-related risk scenarios. Management is able to monitor the risk position and make informed decisions regarding the exposure it is willing to accept. All identified risks have a nominated owner, and senior management and IT management determine the levels of risk that the organisation will tolerate. IT management develops standard measures for assessing risk and defining risk/return ratios. Management budgets for an operational risk management project to reassess risks on a regular basis. A risk management database is established, and part of the risk management processes is beginning to be automated. IT management considers risk
mitigation strategies.

5 **Optimised** when
risk management develops to the stage where a structured, organisationwide process is enforced and well managed. Good practices are applied across the entire organisation. The capture, analysis and reporting of risk management data are highly automated. Guidance is drawn from leaders in the field, and the IT organisation takes part in peer groups to exchange experiences. Risk management is truly integrated into all business and IT operations, is well accepted and extensively involves the users of IT services. Management detects and acts when major IT operational and investment decisions are made without consideration of the risk management plan. Management continually assesses risk mitigation strategies.

PO9 Control Practices

PO9.1 IT Risk Management Framework
Value drivers:
• Consistent approach for IT risk management
• Effective management of IT risks
• Continuous evaluation of current IT risks and threats to the organisation
• Broadened IT risk management approach

Risk drivers:
• IT risks and business risks managed independently
• The impact of an IT risk on the business undetected
• Lack of cost control for risk management
• Each risk seen as a single threat rather than in an overall context
• Ineffective support for risk assessment by senior management

Control practices:
1. Make sure the IT risk management framework fits with the risk management objectives of the enterprise. Use similar risk classification principles and, wherever possible, classify and manage IT risks in a business-driven hierarchy, for example:
   – Strategic
   – Programme
   – Project
   – Operational
2. Define standard scales for IT risk assessment, covering impact and probability aligned with the enterprise risk management framework.
3. Align the IT risk management appetite and tolerance levels with the enterprise risk management framework.

PO9.2 Establishment of Risk Context
Value drivers:
• Effective and efficient use of resources for management of risks
• Alignment of risk management priorities to business needs
• A focus on relevant and significant risks
• Prioritisation of risks

Risk drivers:
• Irrelevant risks considered important
• Significant risks not given appropriate attention
• Inappropriate approach to risk assessment

Control practices:
1. Evaluate risks qualitatively according to their impact (catastrophic, critical, marginal), probability (very likely, probable, improbable) and time frame (imminent, near term, far term), or quantitatively, when appropriate probability data exist.
2. Prioritise risks by separating the 'vital few' from the rest and ranking them based upon a criterion or criteria established by the project team. Techniques for prioritisation include comparison risk ranking, multivoting, and paring to the top 'n' and top five.
3. Perform risk assessment activities considering the context of the IT management processes that are affected.

PO9.3 Event Identification
Value drivers:
• Consistent approach to risk event identification
• Focus on significant risk events

Risk driver:
• Irrelevant risk events identified and focused on whilst more important events are missed

Control practices:
1. Obtain agreement and sign-off from stakeholders of key events and their impacts.
2. Identify potential events that could negatively affect enterprise goals or operations considering results of former audits, inspections and identified incidents, using checklists, workshops, process flow analysis, or other tools and techniques.
3. Identify potential negative impacts that are relevant and significant for the enterprise for each of the selected events. Record and maintain the information in the risk registry, using the enterprise risk management framework terminology.
4. Involve appropriate cross-functional teams in the event and impact identification activity. Depending on the scope of the assessment, these teams may be composed of representatives from the IT, risk management and business functions.
5. Review all potential events as a whole to ensure completeness and to identify interdependencies that could affect impact and probability.

PO9.4 Risk Assessment
Value drivers:
- Improved planning and use of IT risk management skills and resources
- Organisational credibility of IT risk assessment function teams
- Knowledge transfer between risk managers
- Creation of IT asset value awareness

Risk drivers:
- Irrelevant risks considered important
- Each risk seen as a single event rather than in an overall context
- Inability to explain significant risks to management
- Significant risks possibly missed
- Loss of IT assets
- Confidentiality or integrity breach of IT assets

Control practices:
1. Determine the likelihood of identified risks qualitatively (e.g., very likely, probable, improbable) or quantitatively using statistical analysis and probability determinations, based on reasonable sources of information that can be appropriately validated.
2. Determine the material impact on the business of identified risks qualitatively (e.g., catastrophic, critical, marginal) or quantitatively (e.g., impact on revenue or shareholder value).
3. Assess risks inherent in the event and after considering the controls that are in place to identify the residual risks for which a risk response will need to be determined.
4. Document the results of the risk assessment, showing the method followed to come to the conclusions.

PO9.5 Risk Response
Value drivers:
- Effective management of risks
- Consistent approach for risk mitigation
- Cost-effective risk response

Risk drivers:
- Risk responses not effective
- Unidentified residual business risks
- Ineffective use of resources to respond to risks
- Over-reliance on existing poor controls

Control practices:
1. Consider the results of the risk assessment and determine a strategy for mitigating the risks, considering the significance of the risk and the probable cost and benefit of one or more of the options (avoidance, reduction, sharing and acceptance) that aligns with strategic objectives and is in keeping with the enterprise's accepted risk management culture and risk tolerances.
2. Develop a risk action plan to implement the agreed-upon risk response based on a consideration of:
   – Priorities
   – Existing controls that could be improved or modified
   – Practical implementation considerations
   – Any specific legal, regulatory or contractual requirements
   – Probable costs
   – Potential benefits

PO9.6 Maintenance and Monitoring of a Risk Action Plan
Value drivers:
• Effective management of risks
• Continuous evaluation of current risks and threats for the organisation

Risk drivers:
• Risk mitigation controls that do not operate as intended
• Compensating controls that deviate from the identified risks

Control practices:
1. Develop the risk action plan containing prioritised risk responses. Identify priorities, responsibilities, schedules, expected outcome of risk mitigation, costs, benefits, performance measures and the review process to be established.
2. Obtain approval for recommended risk response actions from appropriate authorities. Define and document ownership for approved plan activities, and inform affected parties.
3. Ensure that accepted risks are formally recognised, approved by senior management and recorded.
4. Monitor execution of the action plan, report progress and deviations to senior management, and adjust the plan accordingly.
5. Periodically review the action plan:
   – To ensure that it continues to efficiently and effectively address the IT risks identified
   – In light of any changes to business objectives or relevant IT systems
   – To identify improvement opportunities to the risk assessment and management process

PO9 IT Assurance Guidelines

Test the Control Design
PO 9.1 *IT risk management framework*
• Inspect whether the IT risk management framework aligns with the risk management framework for the organisation (enterprise) and includes business-driven components for strategy, programmes, projects and operations. Review the IT risk classifications to verify that they are based on a common set of characteristics from the enterprise risk management framework. Inspect whether IT risk measurements are standardised and prioritised, and whether they include impact, acceptance of residual risk and probabilities aligned with the enterprise risk management framework.
• Verify whether IT risks are considered in the development and review of IT strategic plans.

PO9.2 *Establishment of risk context*
• Enquire whether and confirm that an appropriate risk context has been defined in line with enterprise risk management policies and principles, and includes processes, such as systems, project management, application software life cycles, management of IT operations and services. Internal and external risk factors should be included.
• Determine whether the IT risk context is communicated and understood.

PO9.3 *Event identification*
• Inspect the process used to identify potential events and determine if all IT processes are included in the analysis. The design of the process should cover internal and external events. Identification of potential events may include results of former audits, inspections and identified incidents, using checklists, workshops and process flow analysis. Trace identified impacts to the risk registry to determine if the registry is complete, current and aligned with the enterprise risk management framework terminology.
• Enquire whether appropriate cross-functional teams are involved in the different event and impact identification activities. Review a sample of the risk registry for relevance of threats, significance of vulnerabilities and importance of impact, and analyse the effectiveness of the process to identify, record and judge risks.

PO9.4 *Risk assessment*
• Walk through the risk management process to determine if inherent and residual risks are defined and documented.
• Enquire whether and confirm that the risk management process assesses identified risks qualitatively and/or quantitatively.
• Inspect project and other documentation to assess the appropriateness of qualitative or quantitative risk assessment.
• Walk through the process to determine if the sources of information used in the analysis are reasonable.
• Inspect the use of statistical analysis and probability determinations to measure the likelihood qualitatively or quantitatively.
• Enquire or inspect whether any correlation between risks is identified. Review any correlation to verify that it exposes significantly different likelihood and impact results arising from such relationship(s).

PO9.5 *Risk response*
- Inspect whether risk assessment results were allocated to a mitigating response to avoid, transfer, reduce, share or accept each risk and align with the mechanisms used to manage risk in the organisation.

PO9.6 *Maintenance and monitoring of a risk action plan*
- Enquire whether accepted risks are formally recognised and recorded in a risk action plan.
- Assess the appropriateness of the elements of the risk management plan.
- Enquire or inspect whether execution, report progress and deviations are monitored.
- Inspect risk responses for appropriate approvals.
- Review actions to verify whether ownership is assigned and documented.
- Inspect whether the risk action plan is effectively maintained and adjusted.

Test the Outcome of the Control Objectives
- Enquire whether the IT risk management tolerance levels are aligned with enterprise risk tolerance levels. Determine whether organisational risk tolerance is used as input for both business and the IT strategy development.
- Enquire whether a process exists to apply enterprise risk tolerance levels to IT risk management decisions. Consider whether benchmarking of the risk assessment framework against similar organisations, appropriate international standards and industry best practices has been performed.
- Test whether risk-related accountability and responsibilities are understood and accepted. Verify that the right skills and necessary resources are available for risk management.
- Enquire through interviews with key staff members involved whether the control mechanism and its purpose, accountability and responsibilities are understood and applied.
- Inspect whether the activities are effectively integrated into IT management processes.
- Inspect whether the identified impacts are relevant and significant for the enterprise, and whether they are either over- or underestimated. Determine whether cross-functional teams contribute to the event analysis process. Verify through interviews and impact reports whether the members of the event identification work group are properly trained on the enterprise risk management framework. Verify whether interdependencies and probabilities are accurately identified during impact assessment. Review any correlation to verify that it exposes significantly different likelihood and impact results arising from such relationships.
- Inspect the risk management process to determine if the sources of information used in the analysis are reasonable.
- Inspect the use of statistical analysis and probability determinations to measure the risk likelihood qualitatively or quantitatively.
- Walk through the process to determine if inherent and residual risks are defined and documented.
- Inspect the risk action plan to determine if it identifies the priorities, responsibilities, schedules, expected outcome, risk mitigation, costs, benefits, performance measures and review process to be established.
- Inspect risk responses for appropriate approvals. Review actions to verify whether ownership is assigned and documented.
- Inspect whether the risk management plan is effectively maintained/adjusted.
- Inspect and review the action plan results to determine if they are performed consistently with the risk framework guidelines and reflect changes to business objective. Review the plan to verify that it is designed in terms of risk avoidance, reduction and sharing. Inspect whether the risk responses to be included are selected on benefit and cost considerations.

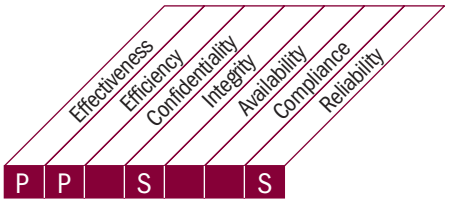
Document the Impact of the Control Weaknesses
- Assess the IT risk management strategy to determine whether it is aligned with the enterprise risk management strategy and organisational risk appetite. Confirm that the potential for unidentified risks, misapplication of IT resources, non-compliance with regulatory requirements and organisational goals has been addressed.
- Assess the accuracy and completeness of event identification, including undetected risk, inefficient and ineffective cost containment, unmitigated risks, uncontrolled aggregated risk levels, loss of organisational assets, harmed reputation, unmet strategic goals, and non-compliance with regulatory requirements.
- Assess the risk action plan's effectiveness at mitigating risks across the enterprise, and examine the correlation of risk and mitigation.
- Review the result of the risk action plan to evaluate effectiveness and ascertain whether owners are responsive and timely in mitigation activities.
- Review risk mitigation activities applied to high-risk threats to assess the effectiveness of the prioritisation.

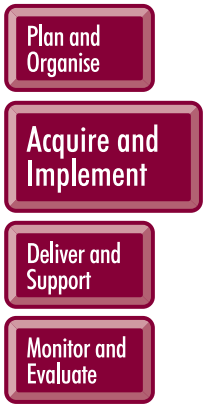
AI2 COBIT COMPONENTS

PROCESS DESCRIPTION

AI2 Acquire and Maintain Application Software

Applications are made available in line with business requirements. This process covers the design of the applications, the proper inclusion of application controls and security requirements, and the development and configuration in line with standards. This allows organisations to properly support business operations with the correct automated applications.





Control over the IT process of

Acquire and maintain application software

that satisfies the business requirement for IT of

aligning available applications with business requirements, and doing so in a timely manner and at a reasonable cost

by focusing on

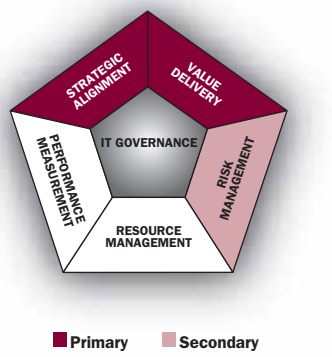
ensuring that there is a timely and cost-effective development process

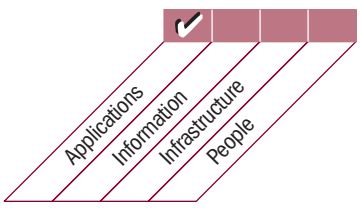
is achieved by

- Translating business requirements into design specifications
- Adhering to development standards for all modifications
- Separating development, testing and operational activities

and is measured by

- Number of production problems per application causing visible downtime
- Percent of users satisfied with the functionality delivered





AI2 Control Objectives

AI2.1 High-level Design
Translate business requirements into a high-level design specification for software acquisition, taking into account the organisation's technological direction and information architecture. Have the design specifications approved by management to ensure that the high-level design responds to the requirements. Reassess when significant technical or logical discrepancies occur during development or maintenance.

AI2.2 Detailed Design
Prepare detailed design and technical software application requirements. Define the criteria for acceptance of the requirements. Have the requirements approved to ensure that they correspond to the high-level design. Perform reassessment when significant technical or logical discrepancies occur during development or maintenance.

AI2.3 Application Control and Auditability
Implement business controls, where appropriate, into automated application controls such that processing is accurate, complete, timely, authorised and auditable.

AI2.4 Application Security and Availability
Address application security and availability requirements in response to identified risks and in line with the organisation's data classification, information architecture, information security architecture and risk tolerance.

AI2.5 Configuration and Implementation of Acquired Application Software
Configure and implement acquired application software to meet business objectives.

AI2.6 Major Upgrades to Existing Systems
In the event of major changes to existing systems that result in significant change in current designs and/or functionality, follow a similar development process as that used for the development of new systems.

AI2.7 Development of Application Software
Ensure that automated functionality is developed in accordance with design specifications, development and documentation standards, QA requirements, and approval standards. Ensure that all legal and contractual aspects are identified and addressed for application software developed by third parties.

AI2.8 Software Quality Assurance
Develop, resource and execute a software QA plan to obtain the quality specified in the requirements definition and the organisation's quality policies and procedures.

AI2.9 Applications Requirements Management
Track the status of individual requirements (including all rejected requirements) during the design, development and implementation, and approve changes to requirements through an established change management process.

AI2.10 Application Software Maintenance
Develop a strategy and plan for the maintenance of software applications.

MANAGEMENT GUIDELINES

AI2 Acquire and Maintain Application Software

From	Inputs
PO2	Data dictionary; data classification scheme; optimised business system plan
PO3	Regular state of technology updates
PO5	Cost-benefits reports
PO8	Acquisition and development standards
PO10	Project management guidelines; detailed project plans
AI1	Business requirements feasibility study
AI6	Change process description

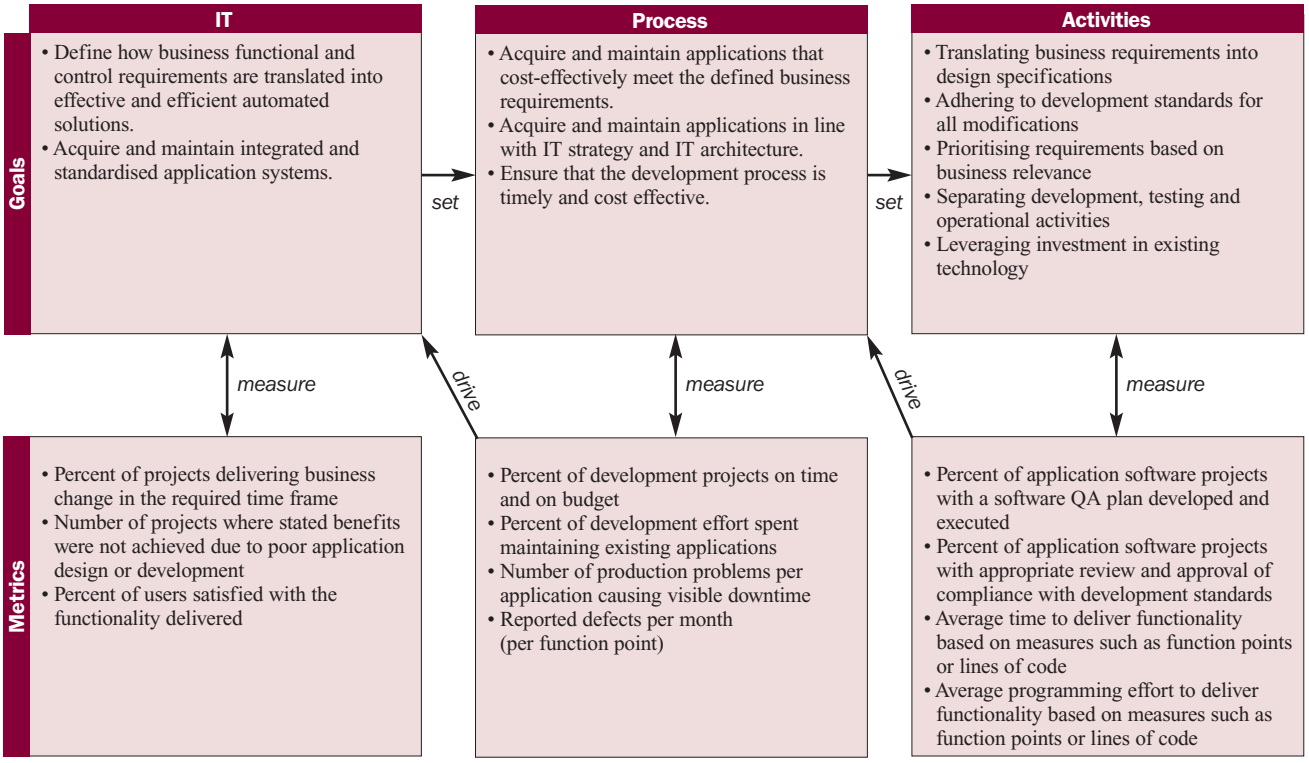
Outputs	To						
Application security controls specification	DS5						
Application and package software knowledge	AI4						
Procurement decisions	AI5						
Initial planned SLAs	DS1						
Availability, continuity and recovery specification	DS3	DS4					

RACI Chart

Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Translate business requirements into high-level design specifications.					C		C	A/R		R	C
Prepare detailed design and technical software application requirements.				I	C	C	C	A/R		R	C
Specify application controls within the design.					R	C		A/R		R	R
Customise and implement acquired automated functionality.					C	C		A/R		R	C
Develop formalised methodologies and processes to manage the application development process.				C		C	C	A	C	R	C
Create a software QA plan for the project.					I		C	R		A/R	C
Track and manage application requirements.								R		A/R	
Develop a plan for the maintenance of software applications.				C		C		A/R		C	

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



AI2 Maturity Model

Management of the process of *Acquire and maintain application software* that satisfies the business requirement for IT of *aligning available applications with business requirements, and doing so in a timely manner and at a reasonable cost* is:

0 **Non-existent** when
there is no process for designing and specifying applications. Typically, applications are obtained based on vendor-driven offerings, brand recognition or IT staff familiarity with specific products, with little or no consideration of actual requirements.

1 **Initial/*Ad Hoc*** when
there is an awareness that a process for acquiring and maintaining applications is required. Approaches to acquiring and maintaining application software vary from project to project. Some individual solutions to particular business requirements are likely to have been acquired independently, resulting in inefficiencies with maintenance and support.

2 **Repeatable but Intuitive** when
there are different, but similar, processes for acquiring and maintaining applications based on the expertise within the IT function. The success rate with applications depends greatly on the in-house skills and experience levels within IT. Maintenance is usually problematic and suffers when internal knowledge is lost from the organisation. There is little consideration of application security and availability in the design or acquisition of application software.

3 **Defined** when
a clear, defined and generally understood process exists for the acquisition and maintenance of application software. This process is aligned with IT and business strategy. An attempt is made to apply the documented processes consistently across different applications and projects. The methodologies are generally inflexible and difficult to apply in all cases, so steps are likely to be bypassed. Maintenance activities are planned, scheduled and co-ordinated.

4 **Managed and Measurable** when
there is a formal and well-understood methodology that includes a design and specification process, criteria for acquisition, a process for testing and requirements for documentation. Documented and agreed-upon approval mechanisms exist to ensure that all steps are followed and exceptions are authorised. Practices and procedures evolve and are well suited to the organisation, used by all staff and applicable to most application requirements.

5 **Optimised** when
application software acquisition and maintenance practices are aligned with the defined process. The approach is component based, with predefined, standardised applications matched to business needs. The approach is enterprisewide. The acquisition and maintenance methodology is well advanced and enables rapid deployment, allowing for high responsiveness and flexibility in responding to changing business requirements. The application software acquisition and implementation methodology is subjected to continuous improvement and is supported by internal and external knowledge databases containing reference materials and good practices. The methodology creates documentation in a predefined structure that makes production and maintenance efficient.

AI2 Control Practices

AI2.1 High-level Design
Value drivers:
- Reduced costs
- Consistency between business requirements and high-level design results
- Improved time to delivery

Risk drivers:
- Dependency on knowledge held by key individuals
- Undefined development scope
- Solutions failing to deliver business requirements
- Solutions not aligned with strategic IT plan, information architecture and technology direction
- High costs of fragmented solutions

Control practices:
1. Establish a high-level design specification that translates the business requirements for the software development based on the organisation's technological direction and information architecture model.
2. Confirm that the design approach and documentation are compliant with the organisation's design standards.
3. Involve appropriately qualified and experienced users in the design process to draw on their expertise and knowledge of existing systems or processes.
4. Confirm that the design is consistent with the business plans, strategies, applicable regulations and IT plans.
5. Ensure that the high-level design is approved and signed off on by IT stakeholders (e.g., human/computer interaction, security and other experts) to ensure that their inputs have been recognised and the design, as a whole, constitutes a solution that the organisation can deliver, operate and maintain. Establish that no project proceeds to the business approval process without appropriate review and sign-off by IT stakeholders.
6. Submit the final high-level design after QA sign-off to the project sponsor/business process owner, and obtain approval and sign-off. Establish that no project proceeds to development without appropriate sign-off by the business.

AI2.2 Detailed Design
Value drivers:
• Reduced costs
• Efficient application coding and maintenance
• Prioritisation on important features
• Avoidance of data redundancy
• Application meeting usability requirements

Risk drivers:
• Processing of invalid transactions
• Increasing costs for system redesign
• Data in application systems processed incorrectly

Control practices:
1. Classify data inputs and outputs according to information architecture and data dictionary standards.
2. Assess the impact on existing applications and infrastructure during the process of gathering requirements and designing the solution, and design appropriate integration approaches. Address integration of the planned application system with existing or planned co-operating applications and infrastructure, including packaged software acquired from third parties. Consider the impact of differing update cycles.
3. Specify the source data collection design, documenting the data that must be collected and validated for processing transactions as well as the methods for validation. Consider data inputs from existing programs, packaged software, external parties, web forms, etc.
4. Define system availability requirements, and design appropriate redundancy, failure recovery and backup processing arrangements.
5. Define file and database requirements for storage, location and retrieval of data. Consider availability, control and auditability, security, and network requirements.
6. Define the processing steps, including specification of transaction types and processing rules incorporating logic transformations or specific calculations. Consider availability, control and auditability, logging, and audit trails.
7. Based on the user requirements and taking into account the different types of recipients, usage, details required, frequency, method of generation and other design details, define the data requirements for all identified outputs. Appropriate design requirements should guarantee the availability, completeness, integrity and confidentiality of output data. Consider the impact of data outputs to other programs, external parties, etc.
8. Design the interface between the user and the system application so that it is easy to use and self-documenting. Consider the impact of system-to-system interface design on infrastructure performance, including the capacity of personal computing devices and network bandwidth and availability.
9. Reassess system design whenever significant technological and/or logical discrepancies occur during design, development and maintenance. Results of the reassessment should be subject to the normal approval cycle.
10. Prepare and document detailed design specifications in accordance with organisational and industry-accepted specification standards and the information architecture.
11. Conduct a design walk-through with IT and business stakeholders before development is initiated, as a part of the sign-off process for the design specifications. Various aids can be used to assist with the sign-off, including prototypes, to aid stakeholder understanding of the final design.

AI2.3 Application Control and Auditability
Value drivers:
• Consistent application controls established
• Ensured data integrity
• Transaction data history able to be validated and reconstructed, if needed

Risk drivers:
• Costly compensating controls
• Data integrity issues
• Gaps between application controls and actual threats and risks
• Processing results and data repositories failing to meet compliance requirements

Control practices:
1. Define all automated application controls (authorisation, input, processing and output) based on business process control requirements provided in the requirements documentation.
2. Define how business processes will need to be adjusted to use the automated control functions provided in purchased/packaged application software.
3. Confirm the design specifications for all automated application controls with IT technical authorities and business process owners, and obtain their approval and sign-off.
4. Confirm that the design includes automated controls within the application that support general control objectives (such as security, data integrity and audit trails), including access control mechanisms and database integrity controls. Confirm that the design has received sign-off from relevant technical design authorities and approval of the business process owner.
5. Assess design specifications of automated application and general controls against internal audit, control, and risk management standards and objectives. Consider the effect of compensating controls outside the application software realm.

AI2.4 Application Security and Availability
Value drivers:
• Preventive and detective security controls established as necessary
• Ensured data confidentiality, integrity and availability
• Maintained system availability for business processing

Risk drivers:
• Undetected security violations
• Costly compensating controls
• Gaps between considered security controls and actual threats and risks

Control practices:
1. Design approaches and solutions to security and availability that adequately meet the defined requirements. These approaches should take into account the organisational security architecture and policies, industry security and privacy best practices, and regulatory and compliance requirements for security and privacy.
2. Consider the security and availability infrastructure already in place. Where possible, build on and extend these capabilities.
3. Consider access rights and privilege management, protection of sensitive information at all stages, authentication and transaction integrity, and automatic recovery.
4. Define how the solutions for security and availability in the infrastructure will be integrated with the application, paying particular attention to transactions, local and wide area networks (e.g., Internet), shared and federated databases, access control mechanisms, load detection, and recovery mechanisms.
5. Confirm the design of security, availability, access management, authentication and protection of transaction integrity with IT technical authorities and, as appropriate, subject matter experts. Obtain their sign-off on and approval of the design. Also confirm with business process owners that the design meets their security and availability requirements using non-technical walk-throughs, where necessary, to confirm understanding.

AI2.5 Configuration and Implementation of Acquired Application Software
Value drivers:
• Acquired system configured to meet business-defined requirements
• Acquired system compliant with existing architecture

Risk drivers:
• Loss of business focus
• Inability to apply future updates effectively
• Reduced system availability and integrity of information

Control practices:
1. Assess the impact of any major upgrade and classify it according to agreed-upon objective criteria (such as business requirements), based on the outcome of analysis of the risk involved (such as impact on existing systems and processes or security), cost-benefit justification and other requirements. Follow normal system development and implementation processes as appropriate for the nature of the change.
2. Consider interoperability with existing applications and databases, appropriate user interfaces, and efficient utilisation of technology resources (e.g., security framework and standards, availability, access management, auditability, networks and storage) in the design specification.
3. Consider the impact of customisation and configuration on the performance and efficiency of the acquired packaged application software and on existing applications. operating systems and other infrastructure.
4. Consider the effect of contractual terms with the vendor on the design of customisation and configuration.
5. Consider the availability of source code for purchased/packaged applications in the customisation and configuration process. Review contractual arrangements with the vendor. Consider escrow arrangements where the source code is not available. Assess the risks in the event that the acquired application packaged software is no longer available at the expiry of a contract or for other reasons.
6. Ensure that testing procedures cover verification of acquired application control objectives (such as functionality, interoperability with existing applications and infrastructure, system performance efficiency, integrated capacity and load stress testing, and data integrity).
7. Conduct a design walk-through with IT and business stakeholders before customisation is initiated, as a part of the sign-off process for the customisation and configuration of application software specifications.
8. Consider whether the implications of customisation and configuration require reassessment of strategies for acquired application packaged software.
9. Obtain approval of business process owners for detailed design specifications for customisation and configuration of application software.
10. Ensure that user and operational manuals (online help) are complete and updated where necessary to account for any customisation or special conditions unique to the implementation.
11. Consider when the effect of cumulative customisations and configurations (including minor changes that were not subjected to formal design specifications) require a high-level reassessment of the acquired solution and associated functionality. Assess whether these changes trigger the development of a detailed design specification for customisation and configuration of the application software. Assess whether these changes restrict the ability of the organisation to adopt vendor upgrades to purchased applications packaged software.

AI2.6 Major Upgrades to Existing Systems
Value drivers:
• Consistent system availability
• Maintained confidentiality, integrity and availability of the processed data
• Cost and quality control for developments
• Maintained compatibility with technical infrastructure

Risk drivers:
• Reduced system availability
• Compromised confidentiality, integrity and availability of processed data
• Lack of cost control for major developments

Control practices:
1. Assess the impact of any major upgrade and classify it according to specified objective criteria (such as business requirements), based on the outcome of analysis of the risk involved (such as impact on existing systems and processes or security), cost-benefit justification and other requirements. Follow normal system development and implementation processes as appropriate for the nature of the change.
2. Obtain agreement on and approval of the implementation of the development and implementation process with the business process sponsor and other affected stakeholders. Ensure that the business process owners understand the effect of designating changes as maintenance or major upgrades.

AI2.7 Development of Application Software
Value drivers:
• Ensuring that business, customer and user needs are met
• Ability to manage and prioritise resources
• Application software creating capabilities for the business
• Application meeting usability requirements

Risk drivers:
• Waste of resources
• Lost focus on business requirements
• High number of failures
• Inability to maintain applications effectively

Control practices:
1. Establish development procedures to ensure that the development of application software adheres to organisational development standards.
2. Ensure that application software is developed based on agreed-upon specifications and business, functional and technical requirements.
3. Establish agreed-upon stages of the development process (development checkpoints). At the end of each stage, facilitate formal discussions of approved criteria with the stakeholders. Obtain approval and sign-off from all stakeholders following successful completion of functionality, performance and quality reviews before finalising stage activities. At the final stage, confirm with IT technical authorities and operations management that the applications are ready and suitable for migration to the production environment.
4. Assess the adequacy of software developed in terms of its compatibility and ease of integration with existing applications and infrastructure.
5. When third-party developers are involved with the applications development, establish that they adhere to contractual obligations and organisational development standards and that licensing requirements have been addressed.
6. Monitor all development activities and track change requests and design, performance and quality reviews, ensuring active participation of all impacted stakeholders, including business process users and IT technology representatives.
7. Ensure that requested changes arising within IT or from the business process owner are tracked.
8. Consider the effect of dynamic, non-sequential development techniques (e.g., rapid application development, extreme programming) on the monitoring of the application development progress and approval of application software by stakeholders.

AI2.8 Software Quality Assurance
Value drivers:
• All-embracing test approach
• Performed tests reflecting the business processes and requirements
• Formally accepted software

Risk drivers:
• Poor software quality
• Retesting of developed software
• Tests failing to reflect current business processes
• Test data misused and compromising corporate security
• Insufficient testing
• Breach of compliance requirements

Control practices:
1. Define a software QA plan. Ensure that the plan includes:
   – Specification of quality criteria
   – Validation and verification processes
   – Definition of how quality will be reviewed
   – Necessary qualifications of quality reviewers
   – Roles and responsibilities for the achievement of quality
   Consider:
   – The effect of embedding quality within the development process
   – The presence or absence of formal review by independent QA teams
   – Ensuring that reviewers are independent from the development team

2. Design a process that monitors the software quality based on:
   – Project requirements
   – Enterprise policies
   – Adherence to site development systems methodologies
   – Quality management procedures and acceptance criteria
3. Employ code inspection, programme walk-throughs and testing of applications. Report on outcomes of the monitoring process and testing to the application software development team and IT management.
4. Monitor all quality exceptions. Ensure that corrective actions are taken. Maintain a record of all reviews, results, exceptions and corrections. Repeat quality reviews, where appropriate, based on the amount of rework and corrective action.

AI2.9 Applications Requirements Management
Value drivers:
• Formally defined requirements and clarified business expectations
• Compliance with the established change management procedures
• An agreed-upon standardised approach for performing changes to the applications in an effective manner

Risk drivers:
• Unauthorised changes
• Changes not applied to the desired systems
• Gaps between expectations and requirements

Control practices:
1. Design a process for standardising, tracking, recording and approving all change requests during development of application systems.
2. Assess the impact of all project change requests, and categorise and prioritise them accordingly.
3. Track changes to requirements for development projects, enabling all stakeholders to monitor, review and approve the changes. Ensure that the outcomes of the change process are fully understood and agreed to by the stakeholders.

AI2.10 Application Software Maintenance
Value drivers:
• Compliance with the established change management procedures
• An agreed-upon standardised approach for performing changes to the applications in an effective manner

Risk drivers:
• Unauthorised changes
• Changes not applied to the desired systems
• Gaps between expectations and requirements
• Reduced system availability

Control practices:
1. Design an effective and efficient process for application software maintenance activities. Prioritise maintenance activities, paying attention to business needs and resource requirements. Ensure that all changes in software comply with the formal change management process, including impact on other systems and infrastructure. Ensure that risk and security requirements and interdependencies are addressed.
2. Monitor all maintenance changes. If appropriate, aggregate maintenance tasks into a single ‘change’ to make management and control easier. Ensure that any major maintenance is categorised and managed as a formal redevelopment.
3. Establish the review and approval of all emergency or any other changes applied without adherence to the formal change process.
4. Ensure that the pattern and volume of maintenance activities are analysed periodically for abnormal trends indicating underlying quality or performance problems.
5. Establish processes to ensure that all maintenance activity is completed successfully and thoroughly. Track maintenance activities to ensure completion. Where necessary, update user systems and operational documentation.

AI2 IT Assurance Guidelines

Test the Control Design

AI2.1 *High-level design*

- Confirm with key IT staff members that a high-level design specification is defined that translates the business requirements for the software development.
- Obtain and review a sample of a project design specification to determine whether it addresses all the business requirements.
- Confirm with key IT staff members whether the project design approach conforms with the organisation's design standard.
- Review high-level design documentation to determine if the organisation's design standards are being followed.
- Review project documentation, such as the project plan and scoping document, to determine if roles and responsibilities of users in the design process are properly included.
- Corroborate management's views regarding user involvement with users/stakeholders to confirm that users'/stakeholders' expertise and knowledge are considered in the design process of new systems.
- Review supporting documents for unambiguous cross-references, including title and date.
- Confirm with stakeholders (IT and business) that they have approved and signed off on the high-level design and that their inputs have been incorporated into the design (e.g., process owners, information owners, security, user representatives).
- Confirm with stakeholders (IT and business) that the high-level design constitutes a solution that the organisation can deliver, operate and maintain (e.g., IT sponsor, business sponsor).

AI2.2 *Detailed design*

- Perform code walk-through and examine documentation associated with data inputs and outputs to determine whether proper storage, location and retrieval methods are implemented according to data dictionary standards.
- Examine information architecture and data dictionary documentation to identify deviations from the data dictionary standards in the programme design.
- Enquire of key staff members whether data dictionary standards are being used, and compare actual performance of data inputs/outputs with responses from key staff members.
- Confirm with key staff members that source data collection design is specified that incorporates computed and stored data.
- Perform code walk-through and inspect plans to confirm that data are collected and validated for processing transactions.
- Confirm with key IT staff members that adequate redundancy, failure recovery and backup arrangements are defined and included in the detailed design specification.
- Review the backup plan and procedures to determine that they adequately address the availability requirements of the new system and are cost-effective.
- Enquire of key IT staff members and review relevant project documentation to determine whether file requirements for storage, location and retrieval of data are defined in the detail design specification.
- Review project documentation to determine if best practices, such as availability, control and auditability, security, and network requirements, are considered.
- Enquire of key staff members and inspect relevant project documentation to determine whether processing steps, including transaction types, processing rules including logic transformations or specific calculations are defined and included in the detailed design specification.
- Enquire of key staff members and inspect relevant project documentation to determine whether integration of system (existing or planned subsystems and acquired packaged software) and infrastructure are addressed continuously throughout the process life cycle.
- Confirm with key IT staff members that all identified output data requirements are properly defined.
- Review detail design documentation to determine that pertinent design details, such as different types of recipients, usage, details required, frequency and method of generation, are considered.
- Review detail design requirement documentation to determine if the availability, completeness, integrity and confidentiality of output data as well as the impact of data outputs to other programmes are appropriately addressed.
- Confirm with key staff members that the interface between the user and the system application is defined and included in the detailed design specification.
- Inspect the detailed design specification to confirm that it adequately addresses user interface requirements.
- Enquire about the system design reassessment procedures that address design changes as a result of significant technological and/or logical discrepancies.
- Review documents such as system design analysis reports or system design change requests to confirm that the system design reassessment procedures are followed (e.g., change in system design needs to be approved by business and IT sponsors).
- Review detailed design specification documentation to determine if it was prepared in conformance with organisation- and industry-accepted specification standards and the information architecture.
- Confirm with IT and business stakeholders that a design walk-through takes place before development commences.

- Review the detailed design specification to confirm that a design walk-through is conducted for all stakeholders and that stakeholder sign-off has been initiated before development (e.g., signature and date or e-mail confirmation).

AI2.3 *Application control and auditability*
- Review the requirements documentation for design of controls to determine that automated application controls are defined based on business process control requirements.
- Review the requirements documentation for design of controls, and identify instances where authorisation, input, processing, output and boundary controls are inadequate.
- Review plans for implementing automated control functions in packaged application software, and determine that business process control requirements are adequately addressed.
- Confirm with business process owners and IT technical design authorities that design specifications for all automated application controls in development or purchased applications are approved.
- Review design specification for all automated application controls in developed or purchased/packaged applications to confirm that they are approved.
- Confirm with project personnel that automated controls have been defined within the application that support general control objectives, such as security, data integrity, audit trails, access control and database integrity controls.
- Perform walk-throughs of application controls in developed and purchased packaged software, trace transactions, and review documentation to ensure that general control objectives (e.g., security, data integrity, audit trails, access control, database integrity controls) are addressed adequately.
- Review project documentation to confirm that design specifications have been assessed against the internal audit, control and risk management standards and objectives.
- Review project documentation to determine if the effects of compensating controls outside the application software realm have been considered.
- Review evidence of high-level review conducted to ensure that automated application and general controls objectives are met (e.g., availability, security, accuracy, completeness, timeliness, authorisation, auditability).

AI2.4 *Application security and availability*
- Enquire with key staff members to assess knowledge and awareness of how solutions for security and availability in the infrastructure will be integrated with the application.
- Review application acquisition, implementation and testing plans to confirm that application security and availability within the integrated environment have been addressed.
- Enquire whether and confirm that availability design has been approved by technical authorities.
- Inspect documentation sign-off by appropriate stakeholders.
- Interview business sponsors and review walk-through documentation to assess understanding and adequacy of availability design; enquire whether the design is likely to meet the security and availability requirements.

AI2.5 *Configuration and implementation of acquired application software*
- Enquire of business process owners and key staff members to determine whether their input and guidance have been solicited and reflected in the application customisation and configuration. Identify instances where business process owner input has not been solicited.
- Confirm with key staff members whether the application software is customised and configured utilising best practice as advised by vendors and in conformance with internal architecture standards.
- Inspect best practices supplied by vendors, compare with the implementation strategy, and identify inappropriate configuration and customisation.
- Confirm with key staff members that testing procedures are in place that cover verification of acquired application control objectives (e.g., functionality, interoperability with existing applications and infrastructure, systems performance efficiency, integration, capacity and load stress testing, data integrity).
- Inspect unit and integration test documentation and walk-through testing procedures to verify the adequacy of the tests.
- Confirm with key staff members that all user and operation manuals are complete and/or updated where necessary. Trace a sample of customisations to user and operational manuals to confirm documentation updates.

AI2.6 *Major upgrades to existing systems*
- Confirm with key staff members and inspect relevant documentation to determine that impact assessment of major upgrades has been made to address the specified objective criteria (such as business requirement), the risk involved (such as impact on existing systems and processes or security), cost-benefit justification and other requirements.
- Inspect relevant documentation to identify deviations from normal development and implementation processes.

- Enquire of business sponsors and other affected stakeholders and inspect relevant documentation to determine whether agreement and approval have been obtained for the development and implementation process.

AI2.7 *Development of application software*
- Confirm with key staff members that all development activity has been established to ensure adherence to development standards and that developed software is based on agreed-upon specifications to meet business, functional and technical requirements.
- Inspect relevant documentation (such as design, code review and walk-throughs) to identify exceptions to specifications and standards.
- Obtain and review assessment documentation of the developed software to confirm adequacy.
- Confirm with key staff members that technical authorities and operations management applications are ready and suitable for migration to the production environment.
- Perform a walk-through of code and identify problems/exceptions.
- Enquire of key staff members to determine compliance with all obligations and requirements.
- Review contractual obligations and licensing requirements relating to third-party developers.

AI2.8 *Software quality assurance*
- Confirm with key staff members that the software QA plan has been defined, including specification of quality criteria, validation and verification processes, and definition of how quality will be reviewed.
- Review the plan for the criteria listed above, and ensure that QA reviews are conducted independent of the development team.
- Confirm with key staff members that a process for monitoring software quality has been designed and established.
- Review relevant documentation to confirm that the process is based on project requirements, enterprise policies, quality management procedures and acceptance criteria.
- Confirm with key staff members that all quality exceptions are identified and that corrective actions are taken.
- Inspect relevant documentation of QA reviews, results, exceptions and corrections to determine that QA reviews are repeated when necessary.

AI2.9 *Applications requirements management*
- Ensure and confirm that changes to individual requirements are monitored, reviewed and approved by the stakeholders involved.
- Inspect relevant documentation to confirm that all changes and status of changes are recorded in the change management system.
- Identify and report changes that are not tracked.

AI2.10 *Application software maintenance*
- Confirm through interviews with key staff members that an effective and efficient process for application software maintenance activities has been designed to ensure uniform application for all changes and can be performed quickly and effectively.
- Review the process documentation to determine that relevant issues (including release planning and control, resource planning, bug fixing and fault correction, minor enhancements, maintenance of documentation, emergency changes, interdependencies with other applications and infrastructure, upgrade strategies, contractual conditions such as support issues and upgrades, periodic review against business needs, risks, and security requirements) are included.
- Confirm with key staff members that all maintenance changes comply with the formal change management process, including impact on existing applications and infrastructure.
- Inspect relevant documentation to confirm that changes are prioritised to identify those that would be better managed as a formal redevelopment. Identify any deviations from the formal change management process.
- Enquire and confirm with key staff whether changes applied without following the formal change management process have been reviewed and approved.
- Review relevant documentation to identify changes that have not been reviewed and approved.
- Enquire and confirm with key staff whether patterns and volume of maintenance activities are assessed periodically for abnormal trends.
- Inspect relevant analytical results documentation to confirm that all underlying quality or performance problems are appropriately analysed and reported.
- Confirm with key staff members that all maintenance activity has been completed successfully and thoroughly.
- Perform a walk-through of maintenance activities to ensure that all tasks and phases have been addressed, including updating user, systems and operational documentation and interdependencies.
- Identify all changes in contractual conditions, business trends or other upgrades that have not been addressed.

Test the Outcome of the Control Objectives
- Review project design documentation to confirm that the design is consistent with business plans, strategies, applicable regulations and IT plans.

- Obtain and review a sample of project sign-off documentation to determine whether the projects have gone through QA sign-off and have proceeded with proper approval of the high-level design by IT and business stakeholders (project sponsors).
- Corroborate with IT management and review relevant documentation to determine if the sampled project design specification aligns with the organisation's technological direction and information architecture.
- Review the integration plan and procedures to determine their adequacy.
- Review project documentation to determine if the impact of the new implementation on existing applications and infrastructure has been assessed and appropriate integration approaches have been considered.
- Review end-of-stage documentation to confirm that all development activities have been monitored and that change requests and quality performance and design reviews have been tracked and considered at formal end-of-stage discussions. Also confirm that stakeholders have been fully represented and that the end-of-stage reviews incorporate approval criteria. Inspect problem logs, review documentation and sign-offs to confirm the adequacy of the development activities and identify deviations.
- Review design documentation to confirm that appropriate solutions and approaches to security and availability are designed to adequately meet the defined requirements and build on or extend the existing infrastructure capability.
- Review QA documentation and fault logs to ensure that all significant quality exceptions are identified and corrective actions are taken. Inspect relevant documentation of QA reviews, results, exceptions and corrections to determine that QA reviews are repeated when necessary.
- Obtain and inspect change requests to determine that they are categorised and prioritised. Confirm with key staff members that the impact of all change requests has been assessed.
- Review change control documentation to confirm that changes applied without following the formal change management process have been reviewed and approved, and to identify changes that have not been reviewed and approved.
- Inspect the risk analysis documentation, and determine whether business and IT risks are identified, examined, assessed and understood by both the business and IT, and that there is evidence that all stakeholders are involved.
- Review the feasibility study documentation to confirm that both technical and economic feasibility have been adequately considered.
- Review quality review documentation, compare with original acceptance criteria, and identify exceptions or deviations from original acceptance criteria.
- Review end-of-stage documentation to confirm that sign-off has been obtained for proposed approaches and/or feedback requiring further feasibility analysis.

Document the Impact of the Control Weaknesses

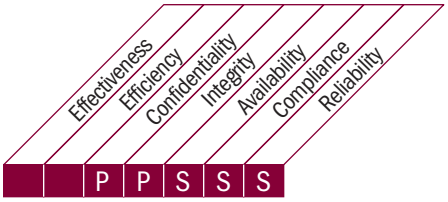
- Identify design specifications that do not reflect user requirements.
- Identify data management requirements that are not consistent with the organisation's data dictionary rules.
- Identify new system development or modification projects that contain inadequately defined file, programme, source data selection, input, user-machine interface, processing, and output and/or controllability requirements.
- Identify designs where security and availability were not adequately considered.
- Identify data integrity design deficiencies.
- Identify test plan requirement deficiencies.
- Identify significant technical and/or logical discrepancies that have occurred during system development or maintenance and did not result in reassessment of the system design and, therefore, went uncorrected or resulted in inefficient, ineffective and uneconomical patches to the system.

DS5 COBIT COMPONENTS

PROCESS DESCRIPTION

DS5 Ensure Systems Security

The need to maintain the integrity of information and protect IT assets requires a security management process. This process includes establishing and maintaining IT security roles and responsibilties, policies, standards, and procedures. Security management also includes performing security monitoring and periodic testing and implementing corrective actions for identified security weaknesses or incidents. Effective security management protects all IT assets to minimise the business impact of security vulnerabilities and incidents.



Control over the IT process of

Ensure systems security

that satisfies the business requirement for IT of

maintaining the integrity of information and processing infrastructure and minimising the impact of security vulnerabilities and incidents

by focusing on

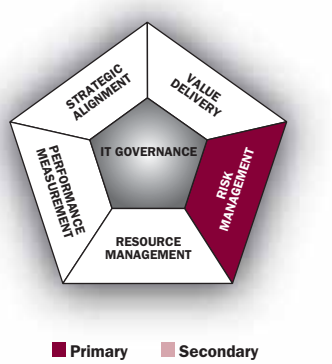
defining IT security policies, plans and procedures, and monitoring, detecting, reporting and resolving security vulnerabilities and incidents

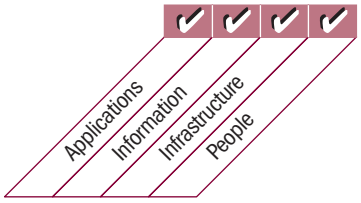
is achieved by

- Understanding security requirements, vulnerabilities and threats
- Managing user identities and authorisations in a standardised manner
- Testing security regularly

and is measured by

- Number of incidents damaging the organisation's reputation with the public
- Number of systems where security requirements are not met
- Number of violations in segregation of duties





DS5 Control Objectives

DS5.1 Management of IT Security
Manage IT security at the highest appropriate organisational level, so the management of security actions is in line with business requirements.

DS5.2 IT Security Plan
Translate business, risk and compliance requirements into an overall IT security plan, taking into consideration the IT infrastructure and the security culture. Ensure that the plan is implemented in security policies and procedures together with appropriate investments in services, personnel, software and hardware. Communicate security policies and procedures to stakeholders and users.

DS5.3 Identity Management
Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT environment, system operations, development and maintenance) are uniquely identifiable. Enable user identities via authentication mechanisms. Confirm that user access rights to systems and data are in line with defined and documented business needs, and that job requirements are attached to user identities. Ensure that user access rights are requested by user management, approved by system owners and implemented by the security-responsible person. Maintain user identities and access rights in a central repository. Deploy cost-effective technical and procedural measures, and keep them current to establish user identification, implement authentication and enforce access rights.

DS5.4 User Account Management
Address requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges with a set of user account management procedures. Include an approval procedure outlining the data or system owner granting the access privileges. These procedures should apply for all users, including administrators (privileged users) and internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information should be contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.

DS5.5 Security Testing, Surveillance and Monitoring
Test and monitor the IT security implementation in a proactive way. IT security should be reaccredited in a timely manner to ensure that the approved enterprise's information security baseline is maintained. A logging and monitoring function will enable the early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed.

DS5.6 Security Incident Definition
Clearly define and communicate the characteristics of potential security incidents so they can be properly classified and treated by the incident and problem management process.

DS5.7 Protection of Security Technology
Make security-related technology resistant to tampering, and do not disclose security documentation unnecessarily.

DS5.8 Cryptographic Key Management
Determine that policies and procedures are in place to organise the generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys to ensure the protection of keys against modification and unauthorised disclosure.

DS5.9 Malicious Software Prevention, Detection and Correction
Put preventive, detective and corrective measures in place (especially up-to-date security patches and virus control) across the organisation to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam).

DS5.10 Network Security
Use security techniques and related management procedures (e.g., firewalls, security appliances, network segmentation, intrusion detection) to authorise access and control information flows from and to networks.

DS5.11 Exchange of Sensitive Data
Exchange sensitive transaction data only over a trusted path or medium with controls to provide authenticity of content, proof of submission, proof of receipt and non-repudiation of origin.

MANAGEMENT GUIDELINES

DS5 Ensure Systems Security

From	Inputs
PO2	Information architecture; assigned data classifications
PO3	Technology standards
PO9	Risk assessment
AI2	Application security controls specification
DS1	OLAs

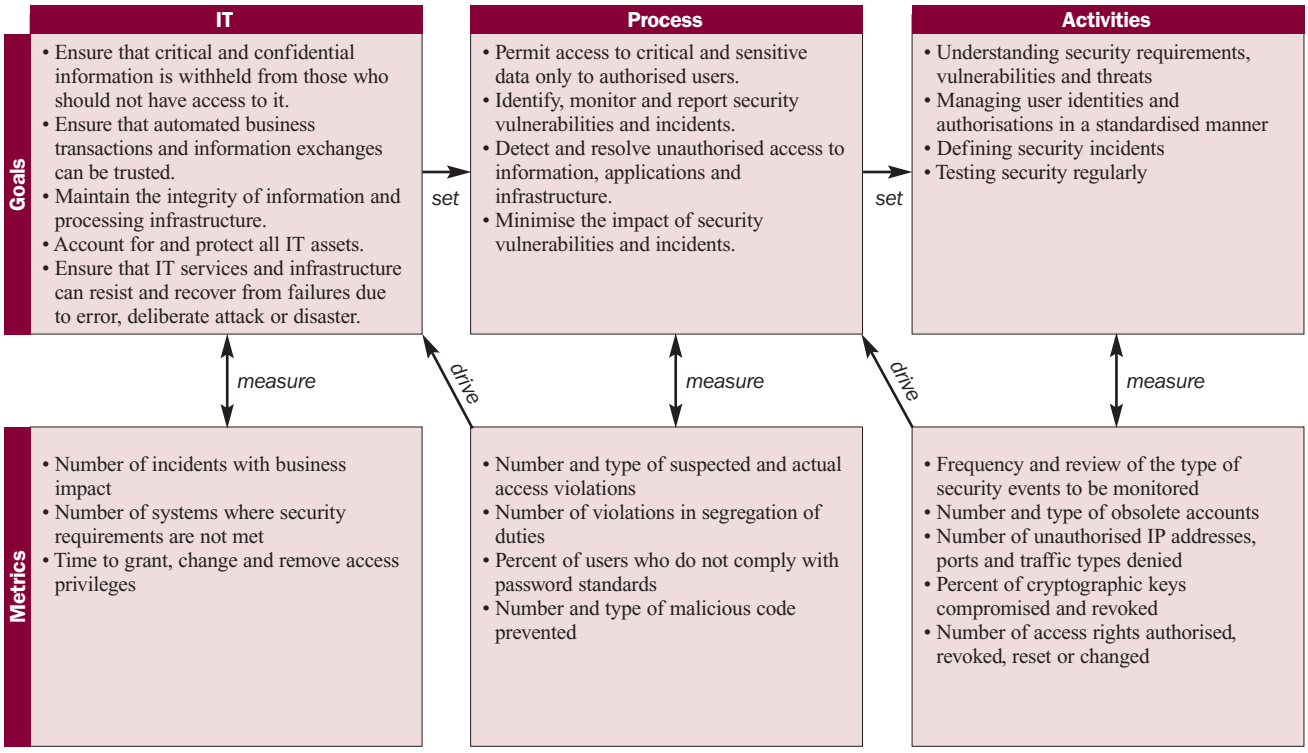
Outputs	To
Security incident definition	DS8
Specific training requirements on security awareness	DS7
Process performance reports	ME1
Required security changes	AI6
Security threats and vulnerabilities	PO9
IT security plan and policies	DS11

RACI Chart

Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Define and maintain an IT security plan.	I	C	C	A	C	C	C	C	I	I	R
Define, establish and operate an identity (account) management process.			I	A	C	R	R	I			C
Monitor potential and actual security incidents.				A	I	R	C	C			R
Periodically review and validate user access rights and privileges.				I	A	C					R
Establish and maintain procedures for maintaining and safeguarding cryptographic keys.				A		R			I		C
Implement and maintain technical and procedural controls to protect information flows across networks.				A	C	C	R	R			C
Conduct regular vulnerability assessments.		I		A	I	C	C	C			R

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



DS5 Maturity Model

Management of the process of *Ensure systems security* that satisfies the business requirements for IT of *maintaining the integrity of information and processing infrastructure and minimising the impact of security vulnerabilities and incidents* is:

0 **Non-existent** when
the organisation does not recognise the need for IT security. Responsibilities and accountabilities are not assigned for ensuring security. Measures supporting the management of IT security are not implemented. There is no IT security reporting and no response process for IT security breaches. There is a complete lack of a recognisable system security administration process.

1 **Initial/*Ad Hoc*** when
the organisation recognises the need for IT security. Awareness of the need for security depends primarily on the individual. IT security is addressed on a reactive basis. IT security is not measured. Detected IT security breaches invoke finger-pointing responses, because responsibilities are unclear. Responses to IT security breaches are unpredictable.

2 **Repeatable but Intuitive** when
responsibilities and accountabilities for IT security are assigned to an IT security co-ordinator, although the management authority of the co-ordinator is limited. Awareness of the need for security is fragmented and limited. Although security-relevant information is produced by systems, it is not analysed. Services from third parties may not address the specific security needs of the organisation. Security policies are being developed, but skills and tools are inadequate. IT security reporting is incomplete, misleading or not pertinent. Security training is available but is undertaken primarily at the initiative of the individual. IT security is seen primarily as the responsibility and domain of IT, and the business does not see IT security as within its domain.

3 **Defined** when
security awareness exists and is promoted by management. IT security procedures are defined and aligned with IT security policy. Responsibilities for IT security are assigned and understood, but not consistently enforced. An IT security plan and security solutions exist as driven by risk analysis. Reporting on security does not contain a clear business focus. *Ad hoc* security testing (e.g., intrusion testing) is performed. Security training is available for IT and the business, but is only informally scheduled and managed.

4 **Managed and Measurable** when
responsibilities for IT security are clearly assigned, managed and enforced. IT security risk and impact analysis is consistently performed. Security policies and procedures are completed with specific security baselines. Exposure to methods for promoting security awareness is mandatory. User identification, authentication and authorisation are standardised. Security certification is pursued for staff members who are responsible for the audit and management of security. Security testing is completed using standard and formalised processes, leading to improvements of security levels. IT security processes are co-ordinated with an overall organisation security function. IT security reporting is linked to business objectives. IT security training is conducted in both the business and IT. IT security training is planned and managed in a manner that responds to business needs and defined security risk profiles. Goals and metrics for security management have been defined but are not yet measured.

5 **Optimised** when
IT security is a joint responsibility of business and IT management, and is integrated with corporate security business objectives. IT security requirements are clearly defined, optimised and included in an approved security plan. Users and customers are increasingly accountable for defining security requirements, and security functions are integrated with applications at the design stage. Security incidents are promptly addressed with formalised incident response procedures supported by automated tools. Periodic security assessments are conducted to evaluate the effectiveness of the implementation of the security plan. Information on threats and vulnerabilities is systematically collected and analysed. Adequate controls to mitigate risks are promptly communicated and implemented. Security testing, root cause analysis of security incidents and proactive identification of risk are used for continuous process improvements. Security processes and technologies are integrated organisationwide. Metrics for security management are measured, collected and communicated. Management uses these measures to adjust the security plan in a continuous improvement process.

DS5 Control Practices

DS5.1 Management of IT Security
Value drivers:
• Critical IT assets protected
• IT security strategy supporting business needs
• IT security strategy aligned with the overall business plan
• Appropriately implemented and maintained security practices consistent with applicable laws and regulations

Risk drivers:
• Lack of IT security governance
• Misaligned IT and business objectives
• Unprotected data and information assets

Control practices:
1. Define a charter for IT security, defining for the security management function:
   – Scope and objectives for the security management function
   – Responsibilities
   – Drivers (e.g., compliance, risk, performance)
2. Confirm that the board, executive management and line management direct the policy development process to ensure that the IT security policy reflects the requirements of the business.
3. Set up an adequate organisational structure and reporting line for information security, ensuring that the security management and administration functions have sufficient authority. Define the interaction with enterprise functions, particularly the control functions such as risk management, compliance and audit.
4. Implement an IT security management reporting mechanism, regularly informing the board and business and IT management of the status of IT security so that appropriate management actions can be taken.

DS5.2 IT Security Plan
Value drivers:
• The IT security plan satisfying business requirements and covering all risks to which the business is exposed
• Investments in IT security managed in a consistent manner to enable the security plan
• Security policies and procedures communicated to stakeholders and users
• Users aware of the IT security plan

Risk drivers:
• IT security plan not aligned with business requirements
• IT security plan not cost effective
• Business exposed to threats not covered in the strategy
• Gaps between planned and implemented IT security measures
• Users not aware of the IT security plan
• Security measures compromised by stakeholders and users

Control practices:
1. Define and maintain an overall IT security plan that includes:
   – A complete set of security policies and standards in line with the established information security policy framework
   – Procedures to implement and enforce the policies and standards
   – Roles and responsibilities
   – Staffing requirements
   – Security awareness and training
   – Enforcement practices
   – Investments in required security resources
2. Collect information security requirements from IT tactical plans (PO1), data classification (PO2), technology standards (PO3), security and control policies (PO6), risk management (PO9), and external compliance requirements (ME3) for integration into the overall IT security plan.
3. Translate the overall IT security plan into enterprise information security baselines for all major platforms and integrate it into the configuration baseline (DS9).

4. Provide information security requirements and implementation advice to other processes, including the development of SLAs and OLAs (DS1 and DS2), automated solution requirements (AI1), application software (AI2), and IT infrastructure components (AI3).
5. Communicate to all stakeholders and users in a timely and regular fashion on updates of the information security strategy, plans, policies and procedures.

DS5.3 Identity Management
Value drivers:
• Effective implementation of changes
• Proper investigation of improper access activity
• Secure communication ensuring approved business transactions

Risk drivers:
• Unauthorised changes to hardware and software
• Access management failing business requirements and compromising the security of business-critical systems
• Unspecified security requirements for all systems
• Segregation-of-duty violations
• Compromised system information

Control practices:
1. Establish and communicate policies and procedures to uniquely identify, authenticate and authorise access mechanisms and access rights for all users on a need-to-know/need-to-have basis, based on predetermined and preapproved roles. Clearly state accountability of any user for any action on any of the systems and/or applications involved.
2. Ensure that roles and access authorisation criteria for assigning user access rights take into account:
   – Sensitivity of information and applications involved (data classification)
   – Policies for information protection and dissemination (legal, regulatory, internal policies and contractual requirements)
   – Roles and responsibilities as defined within the enterprise
   – The need-to-have access rights associated with the function
   – Standard but individual user access profiles for common job roles in the organisation
   – Requirements to guarantee appropriate segregation of duties
3. Establish a method for authenticating and authorising users to establish responsibility and enforce access rights in line with sensitivity of information and functional application requirements and infrastructure components, and in compliance with applicable laws, regulations, internal policies and contractual agreements.
4. Define and implement a procedure for identifying new users and recording, approving and maintaining access rights. This needs to be requested by user management, approved by the system owner and implemented by the responsible security person.
5. Ensure that a timely information flow is in place that reports changes in jobs (i.e., people in, people out, people change). Grant, revoke and adapt user access rights in co-ordination with human resources and user departments for users who are new, who have left the organisation, or who have changed roles or jobs.

DS5.4 User Account Management
Value drivers:
• Consistently managed and administered user accounts
• Rules and regulations for all kinds of users
• Timely discovery of security incidents
• Protection of IT systems and confidential data from unauthorised users

Risk drivers:
• Security breaches
• Users failing to comply with security policy
• Incidents not solved in a timely manner
• Failure to terminate unused accounts in a timely manner, thus impacting corporate security

Control practices:
1. Ensure that access control procedures include but are not limited to:
   – Using unique user IDs to enable users to be linked to and held accountable for their actions
   – Awareness that the use of group IDs results in the loss of individual accountability and are permitted only when justified for business or operational reasons and compensated by mitigating controls. Group IDs must be approved and documented.
   – Checking that the user has authorisation from the system owner for the use of the information system or service, and the level of access granted is appropriate to the business purpose and consistent with the organisational security policy

– A procedure to require users to understand and acknowledge their access rights and the conditions of such access
– Ensuring that internal and external service providers do not provide access until authorisation procedures have been completed
– Maintaining a formal record, including access levels, of all persons registered to use the service
– A timely and regular review of user IDs and access rights
2. Ensure that management reviews or reallocates user access rights at regular intervals using a formal process. User access rights should be reviewed or reallocated after any job changes, such as transfer, promotion, demotion or termination of employment. Authorisations for special privileged access rights should be reviewed independently at more frequent intervals.

DS5.5 Security Testing, Surveillance and Monitoring
Value drivers:
• Staff experienced in security testing and monitoring of IT systems
• Regularly reviewed security level
• Deviations from business requirements highlighted
• Security breaches detected proactively

Risk drivers:
• Misuse of users' accounts, compromising organisational security
• Undetected security breaches
• Unreliable security logs

Control practices:
1. Implement monitoring, testing, reviews and other controls to:
– Promptly prevent/detect errors in the results of processing
– Promptly identify attempted, successful and unsuccessful security breaches and incidents
– Detect security events and thereby prevent security incidents by using detection and prevention technologies
– Determine whether the actions taken to resolve a breach of security are effective
2. Conduct effective and efficient security testing procedures at regular intervals to:
– Verify that identity management procedures are effective
– Verify that user account management is effective
– Validate that security-relevant system parameter settings are defined correctly and are in compliance with the information security baseline
– Validate that network security controls/settings are configured properly and are in compliance with the information security baseline
– Validate that security monitoring procedures are working properly
– Consider, where necessary, obtaining expert reviews of the security perimeter

DS5.6 Security Incident Definition
Value drivers:
• Proactive security incident detection
• Reporting of security breaches on a defined and documented level
• Identified ways of communication for security incidents

Risk drivers:
• Undetected security breaches
• Lack of information for performing counterattacks
• Missing classification of security breaches

Control practices:
1. Describe what a security incident is considered to be. Document within the characteristics a limited number of impact levels to allow commensurate response. Communicate and distribute this information, or relevant parts thereof, to identified people who need to be notified.
2. Ensure that security incidents and appropriate follow-up actions, including root cause analysis, follow the existing incident and problem management processes.
3. Define measures to protect confidentiality of information related to security incidents.

DS5.7 Protection of Security Technology
Value drivers:
• Corporate security technology protected
• Reliable information secured
• Corporate assets protected

Risk drivers:
• Exposure of information
• Breach of trust with other organisations
• Violations of legal and regulatory requirements

Control practices:
1. Ensure that all hardware, software and facilities related to the security function and controls, e.g., security tokens and encryptors, are tamperproof.
2. Secure security documentation and specifications to prevent unauthorised access. However, do not make security of systems reliant solely on secrecy of security specifications.
3. Make the security design of dedicated security technology (e.g., encryption algorithms) strong enough to resist exposure, even if the security design is made available to unauthorised individuals.
4. Evaluate the protection mechanisms on a regular basis (at least annually) and perform updates to the protection of the security technology, if necessary.

DS5.8 Cryptographic Key Management
Value drivers:
• Defined and documented key management
• Keys handled in a secure manner
• Secure communication

Risk drivers:
• Keys misused by unauthorised parties
• Registration of non-verified users, thus compromising system security
• Unauthorised access to cryptographic keys

Control practices:
1. Ensure that there are appropriate procedures and practices in place for the generation, storage and renewal of the root key, including dual custody and observation by witnesses.
2. Make sure that procedures are in place to determine when a root key renewal is required (e.g., the root key is compromised or expired).
3. Create and maintain a written certification practice statement that describes the practices that have been implemented in the certification authority, registration authority and directory when using a public-key-based encryption system.
4. Create cryptographic keys in a secure manner. When possible, enable only individuals not involved with the operational use of the keys to create the keys. Verify the credentials of key requestors (e.g., registration authority).
5. Ensure that cryptographic keys are distributed in a secure manner (e.g., offline mechanisms) and stored securely, that is:
   – In an encrypted form regardless of the storage media used (e.g., write-once disk with encryption)
   – With adequate physical protection (e.g., sealed, dual custody vault) if stored on paper
6. Create a process that identifies and revokes compromised keys. Notify all stakeholders as soon as possible of the compromised key.
7. Verify the authenticity of the counterparty before establishing a trusted path.

DS5.9 Malicious Software Prevention, Detection and Correction
Value drivers:
• System security ensured by proactive malware protection
• Ensured system integrity
• Timely detection of security threats

Risk drivers:
• Exposure of information
• Violations of legal and regulatory requirements
• Systems and data that are prone to virus attacks
• Ineffective countermeasures

Control practices:
1. Establish, document, communicate and enforce a malicious software prevention policy in the organisation. Ensure that people in the organisation are aware of the need for protection against malicious software, and their responsibilities relative to same.
2. Install and activate malicious software protection tools on all processing facilities, with malicious software definition files that are updated as required (automatically or semi-automatically).
3. Distribute all protection software centrally (version and patch-level) using centralised configuration and change management.
4. Regularly review and evaluate information on new potential threats.
5. Filter incoming traffic, such as e-mail and downloads, to protect against unsolicited information (e.g., spyware, phishing e-mails).

DS5.10 Network Security
Value drivers:
• Corporate security technology protected
• Reliable information secured
• Corporate assets protected
• Network security managed in a consistent manner

Risk drivers:
• Failure of firewall rules to reflect the organisation's security policy
• Undetected unauthorised modifications to firewall rules
• Compromised overall security architecture
• Security breaches not detected in a timely manner

Control practices:
1. Establish, maintain, communicate and enforce a network security policy (e.g., provided services, allowed traffic, types of connections permitted) that is reviewed and updated on a regular basis (at least annually).
2. Establish and regularly update the standards and procedures for administering all networking components (e.g., core routers, DMZ, VPN switches, wireless).
3. Properly secure network devices with special mechanisms and tools (e.g., authentication for device management, secure communications, strong authentication mechanisms). Implement active monitoring and pattern recognition to protect devices from attack.
4. Configure operating systems with minimal features enabled (e.g., features that are necessary for functionality and are hardened for security applications). Remove all unnecessary services, functionalities and interfaces (e.g., graphical user interface [GUI]). Apply all relevant security patches and major updates to the system in a timely manner.
5. Plan the network security architecture (e.g., DMZ architectures, internal and external network, IDS placement and wireless) to address processing and security requirements. Ensure that documentation contains information on how traffic is exchanged through systems and how the structure of the organisation's internal network is hidden from the outside world.
6. Subject devices to reviews by experts who are independent of the implementation or maintenance of the devices.

DS5.11 Exchange of Sensitive Data
Value drivers:
• Trusted ways of communications
• Reliable information exchange
• System and data integrity safeguarded

Risk drivers:
• Sensitive information exposed
• Inadequate physical security measures
• Unauthorised external connections to remote sites
• Disclosure of corporate assets and sensitive information accessible for unauthorised parties

Control practices:
1. Determine by using the established information classification scheme how the data should be protected when exchanged.
2. Apply appropriate application controls to protect the data exchange.
3. Apply appropriate infrastructure controls, based on information classification and technology in use, to protect the data exchange.

DS5 IT Assurance Guidelines

Test the Control Design

DS5.1 *Management of IT security*
- Determine if a security steering committee exists, with representation from key functional areas, including internal audit, HR, operations, IT security and legal.
- Determine if a process exists to prioritise proposed security initiatives, including required levels of policies, standards and procedures.
- Enquire whether and confirm that an information security charter exists.
- Review and analyse the charter to verify that it refers to the organisational risk appetite relative to information security and that the charter clearly includes:
  - Scope and objectives of the security management function
  - Responsibilities of the security management function
  - Compliance and risk drivers
- Enquire whether and confirm that the information security policy covers the responsibilities of board, executive management, line management, staff members and all users of the enterprise IT infrastructure, and that it refers to detailed security standards and procedures.
- Enquire whether and confirm that a detailed security policy, standards and procedures exist. Examples of policies, standards and procedures include:
  - Security compliance policy
  - Management risk acceptance (security non-compliance acknowledgement)
  - External communications security policy
  - Firewall policy
  - E-mail security policy
  - An agreement to comply with IS policies
  - Laptop/desktop computer security policy
  - Internet usage policy
- Enquire whether and confirm that an adequate organisational structure and reporting line for information security exist, and assess if the security management and administration functions have sufficient authority.
- Enquire whether and confirm that a security management reporting mechanism exists that informs the board, business and IT management of the status of information security.

DS5.2 *IT security plan*
- Determine the effectiveness of the collection and integration of information security requirements into an overall IT security plan that is responsive to the changing needs of the organisation.
- Verify that the IT security plan considers IT tactical plans (PO1), data classification (PO2), technology standards (PO3), security and control policies (PO6), risk management (PO9), and external compliance requirements (ME3).
- Determine if a process exists to periodically update the IT security plan, and if the process requires appropriate levels of management review and approval of changes.
- Determine if enterprise information security baselines for all major platforms are commensurate with the overall IT security plan, if the baselines have been recorded in the configuration baseline (DS9) central repository, and if a process exists to periodically update the baselines based on changes in the plan.
- Determine if the IT security plan includes the following:
  - A complete set of security policies and standards in line with the established information security policy framework
  - Procedures to implement and enforce the policies and standards
  - Roles and responsibilities
  - Staffing requirements
  - Security awareness and training
  - Enforcement practices
  - Investments in required security resources
- Determine if a process exists to integrate information security requirements and implementation advice from the IT security plan into other processes, including the development of SLAs and OLAs (DS1-DS2), automated solution requirements (AI1), application software (AI2), and IT infrastructure components (AI3).

DS5.3 *Identity management*
- Determine if security practices require users and system processes to be uniquely identifiable and systems to be configured to enforce authentication before access is granted.
- If predetermined and preapproved roles are utilised to grant access, determine if the roles clearly delineate responsibilities based on least privileges and ensure that the establishment and modification of roles are approved by process owner management.
- Determine if access provisioning and authentication control mechanisms are utilised for controlling logical access across all users, system processes and IT resources, for in-house and remotely managed users, processes and systems.

DS5.4 *User account management*
- Determine if procedures exist to periodically assess and recertify system and application access and authorities.
- Determine if access control procedures exist to control and manage system and application rights and privileges according to the organisation's security policies and compliance and regulatory requirements.
- Determine if systems, applications and data have been classified by levels of importance and risk, and if process owners have been identified and assigned.
- Determine if user provisioning policies, standards and procedures extend to all system users and processes, including vendors, service providers and business partners.

DS5.5 *Security testing, surveillance and monitoring*
- Enquire whether and confirm that an inventory of all network devices, services and applications exists and that each component has been assigned a security risk rating.
- Determine if security baselines exist for all IT utilised by the organisation.
- Determine if all organisation-critical, higher-risk network assets are routinely monitored for security events.
- Determine if the IT security management function has been integrated within the organisation's project management initiatives to ensure that security is considered in development, design and testing requirements, to minimise the risk of new or existing systems introducing security vulnerabilities.

DS5.6 *Security incident definition*
- Determine if a computer emergency response team (CERT) exists to recognise and effectively manage security emergencies. The following areas should exist as part of an effective CERT process:
  - Incident handling—General and specific procedures and other requirements to ensure effective handling of incidents and reported vulnerabilities
  - Vendor relations—The role and responsibilities of vendors in incident prevention and follow-up, software flaw correction, and other areas
  - Communications—Requirements, implementation and operation of emergency and routine communications channels amongst key members of management
  - Legal and criminal investigative issues—Issues driven by legal considerations and the requirements or constraints resulting from the involvement of criminal investigative organisations during an incident
  - Constituency relations—Response centre support services and methods of interaction with constituents, including training and awareness, configuration management, and authentication
  - Research agenda and interaction—Identification of existing research activities and requirements and rationale for needed research relating to response centre activities
  - Model of the threat—Development of a basic model that characterises potential threats and risks to help focus risk reduction activities and progress in those activities
  - External issues—Factors that are outside the direct control of the company (e.g., legislation, policy, procedural requirements) but that could affect the operation and effectiveness of the company's activities
- Determine if the security incident management process appropriately interfaces with key organisation functions, including the help desk, external service providers and network management.
- Evaluate if the security incident management process includes the following key elements:
  - Event detection
  - Correlation of events and evaluation of threat/incident
  - Resolution of threat, or creation and escalation work order
  - Criteria for initiating the organisation's CERT process
  - Verification and required levels of documentation of the resolution
  - Post-remediation analysis
  - Work order/incident closure

DS5.7 *Protection of security technology*
- Enquire whether and confirm that policies and procedures have been established to address security breach consequences (specifically to address controls to configuration management, application access, data security and physical security requirements).
- Inspect the control records granting and approving access and logging unsuccessful attempts, lockouts, authorised access to sensitive files and/or data, and physical access to facilities.
- Enquire whether and confirm that the security design features facilitate password rules (e.g., maximum length, characters, expiration, reuse).
- Enquire whether and confirm that the control requires annual management reviews of security features for physical and logical access to files and data.
- Verify that access is authorised and appropriately approved.
- Inspect security reports generated from system tools preventing network penetration vulnerability attacks.

DS5.8 *Cryptographic key management*
- Determine if a defined key life cycle management process exists. The process should include:
  - Minimum key sizes required for the generation of strong keys
  - Use of required key generation algorithms
  - Identification of required standards for the generation of keys
  - Purposes for which keys should be used and restricted
  - Allowable usage periods or active lifetimes for keys
  - Acceptable methods of key distribution
  - Key backup, archival and destruction
- Assess if controls over private keys exist to enforce their confidentiality and integrity. Consideration should be given to the following:
  - Storage of private signing keys within secure cryptographic devices (e.g., FIPS 140-1, ISO 15782-1, ANSI X9.66)
  - Private keys not exported from a secure cryptographic module
  - Private keys backed up, stored and recovered only by authorised personnel using dual control in a physically secured environment
- Enquire whether and confirm that the organisation has implemented information classification and associated protective controls for information that account for the organisation's needs for sharing or restricting information and the organisational impacts associated with such needs.
- Determine if procedures are defined to ensure that information labelling and handling is performed in accordance with the organisation's information classification scheme.

DS5.9 *Malicious software prevention, detection and correction*
- Enquire whether and confirm that a malicious software prevention policy is established, documented and communicated throughout the organisation.
- Ensure that automated controls have been implemented to provide virus protection and that violations are appropriately communicated.
- Enquire of key staff members whether they are aware of the malicious software prevention policy and their responsibility for ensuring compliance.
- From a sample of user workstations, observe whether a virus protection tool has been installed and includes virus definition files and the last time the definitions were updated.
- Enquire whether and confirm that the protection software is centrally distributed (version and patch-level) using a centralised configuration and change management process.
- Review the distribution process to determine the operating effectiveness.
- Enquire whether and confirm that information on new potential threats is regularly reviewed and evaluated and, as necessary, manually updated to the virus definition files.
- Review the review and evaluation process to determine operating effectiveness.
- Enquire whether and confirm that incoming e-mail is filtered appropriately against unsolicited information.
- Review the filtering process to determine operating effectiveness, or review the automated process established for filtering purposes.

DS5.10 *Network security*
- Enquire whether and confirm that a network security policy (e.g., provided services, allowed traffic, types of connections permitted) has been established and is maintained.
- Enquire whether and confirm that procedures and guidelines for administering all critical networking components (e.g., core routers, DMZ, VPN switches) are established and updated regularly by the key administration personnel, and changes to the documentation are tracked in the document history.

DS5.11 *Exchange of sensitive data*
- Enquire whether and confirm that data transmissions outside the organisation require encrypted format prior to transmission.
- Enquire whether and confirm that corporate data are classified according to exposure level and classification scheme (e.g., confidential, sensitive).
- Enquire whether and confirm that sensitive data processing is controlled through application controls that validate the transaction prior to transmission.
- Review that the application logs or halts processing for invalid or incomplete transactions.

Test the Outcome of the Control Objectives
- Through inquiry and observation, determine if the security management function effectively interacts with key enterprise functions, including areas such as risk management, compliance and audit.
- Review the process for identifying and responding to security incidents, selecting a sample of recorded incidents. Through inquiry and review of supporting documentation, determine whether appropriate management action has been taken to resolve the incident.
- Select a sample of employees and determine if computer usage and confidentiality (non-disclosure) agreements have been signed as part of their initial terms and conditions of employment.
- Review the IT security strategy, plans, policies and procedures to determine their relevance to the organisation's current IT landscape, and determine when they were last reviewed and updated.
- Review the IT security strategy, plans, policies and procedures, and verify that they reflect the data classification.
- Interview stakeholders and users on their knowledge of the IT security strategy, plans, policies and procedures, and determine if stakeholders and users find them to be relevant to risks and organisational practices.
- Ask executive management about any recent or planned changes to the organisation (e.g., business unit acquisitions/dispositions, new systems, changes in regulatory environment), and determine if the IT security plan is properly aligned.
- Determine if security processes have been implemented to uniquely identify and control the actions of all users and processes through review of system (development, test and production systems) and application accounts, job queues and services, and security software mode settings.
- Through a sample of access control lists (ACLs), determine whether the security provisioning process appropriately considers the following:
  – Sensitivity of the information and applications involved (data classification)
  – Policies for information protection and dissemination (legal, regulatory and contractual requirements)
  – The 'need-to-have' of the function
  – Standard user access profiles for common job roles in the organisation
  – The need for segregation for the access rights involved
  – Data owner and management's authorisation for access
  – The documentation of identity and access rights in a central repository
  – Creation, communication and change of initial passwords
- Through inquiry and review of sampled ACLs, determine if a process exists for resolving access provisioning requests that are not commensurate with established security authentication practices and roles.
- Determine if a risk assessment process was utilised to identify possible segregation of duties and if an escalation process was utilised to obtain added levels of management authorisation.
- Determine if authentication and authorisation mechanisms exist to enforce access rights according to the sensitivity and criticality of information (e.g., password, token, digital signature).
- Determine if trust relationships enforce comparable security levels and maintain user and process identities.
- Select a sample of user and system accounts and a sample ACL to determine existence of the following:
  – Clearly defined requested role and/or privileges
  – Business justification for assignment
  – Data owner and management authorisation
  – Business/risk justification and management approval for non-standard requests
  – Access requested commensurate with job function/role and required segregation of duties
  – Documentation evidencing adherence to and completion of the provisioning process
- Obtain from HR a sample of employee transfers and terminations and, through review of system account profiles and/or ACLs, determine if access has been appropriately altered and/or revoked in a timely manner.
- Select a sample of critical network devices and system services, and determine if access control mechanisms have been routinely evaluated and tested to confirm their operational effectiveness.
- Select a sample of critical network devices and system services, and determine if they have been routinely monitored for existence of security incidents.
- Sample security baselines and determine if they are appropriately aligned to the organisation's risk profile and levels of accepted risk and if they take into account common risks and vulnerabilities (i.e., conform to leading practices).

- Select a sample of IT devices and determine their compliance with established security baselines. For deviations from baselines, determine if a risk assessment was performed and if management approved the deviation from the baseline.
- Determine if a security review process has been integrated into the organisation's acquisition and implementation processes (AI) and delivery and support processes (DS), requiring security management's involvement and approval of any IT changes that would impact the design or operation systems security. The review process should consider:
  – Overall technology architecture
  – Database access and security design
  – Protocol, port and socket usage
  – Required services
  – User remote access and modem requirements
  – Server-to-server authentication and encryption
  – Scalability, availability and redundancy
  – Session management and cookie usage
  – Administrative capabilities
  – User ID and password management
  – Audit trails and logging/reporting
- Determine if security audit trails capture user identification (ID), type of event, date and time, success or failure indication, origination of event, and the identity or the name of the affected object. Logged events should include accesses to sensitive data, actions by administrative and privileged accounts, initialisation of audit logs, and modification of system-level objects.
- Inspect and review documents supporting the recording, analysis and resolution of potential security incidents, and perform the following steps:
  – Understand the methods used to categorise incidents and identify actionable threats.
  – Identify specific logged security incidents, and inquire as to the nature and disposition of the incident.
- Inspect documentation evidencing the process used to match the organisation's network device inventory to published vulnerabilities for the purpose of verifying that all devices are at current release and security patch levels.
- Determine if formal management responsibilities and procedures exist throughout the key management life cycle, including changes to encryption equipment, software and operating procedures.
- For a sample of new keys, determine if key pairs have been generated in accordance with industry standards and compliance or regulatory requirements (e.g., ISO 15782-1, FIPS 140-1, ANSI X9.66) and if documentation evidences the existence of split-knowledge and dual-control keys (requiring two or three people, each knowing only his/her part of the key, to reconstruct the whole key).
- For a sample of expired keys, determine if documentation exists evidencing the complete destruction of keys at the end of the key-pair life cycle.
- Review maintenance records evidencing that cryptographic hardware is routinely tested.
- Obtain a list of individuals who have access to cryptographic hardware, software and keys, and determine if access is limited to properly authorised individuals responsible for the creation and injection of keys.
- Determine if key custodians formally acknowledge, understand and accept their key custodian responsibilities.
- Determine if encryption keys are generated, stored and used in a manner such that the keys and their components are known only to authorised custodians.
- For keys received from third-party vendors, determine if they are sent in separate parts by different carriers on different dates, and if each part of the key is stored in a separate safe, for which the combination is known by a separate key officer.
- Assess the system security features to evaluate whether proactive controls have been established to protect from malicious security attacks.
- Assess whether the data/system protection software is centrally distributed throughout the network environment.
- Assess the control features for filtering incoming traffic against unsolicited information.
- Select a sample of critical network devices, and confirm that the devices are properly secured with special mechanisms and tools (e.g., authentication for device management, secure communications, strong authentication mechanisms) and that active monitoring and pattern recognition are in place to protect devices from attack.
- Select a sample of network devices, and determine if the devices have been configured with minimal features enabled (e.g., features that are necessary for functionality and hardened for security applications); all unnecessary services, functionalities and interfaces have been removed; and all relevant security patches and major updates are applied to the system in a timely manner before going to production.
- Select a sample of new network devices or changes to existing network devices and determine that the organisation's Acquire and Implement (AI) process controls and Deliver and Support (DS) process controls have been followed.
- Select a sample of firewall devices, and review ACLs for the following:
  – Access rules effectively segregating trusted and non-trusted network segments
  – Documentation evidencing the business purpose and management's approval of rules

  – Configurations following management-approved baselines
  – Devices that are current on version and patch release levels
- Determine if encryption is utilised for all non-console administrative access, such as SSH, VPN or SSL/TLS.
- Assess whether automated controls safeguard the data and systems, such that data are transmitted through reliable sources.
- Determine if user management periodically reviews user profiles and access rights to ensure the adequacy of access rights and requirements for segregation of duties.
- Verify that direct access to data is prevented or, where required, controlled and documented accordingly.
- Verify that the quality requirements for passwords are defined and enforced by systems.

Document the Impact of the Control Weaknesses
- Determine the level of security consciousness within the organisation by reviewing functional and operational documentation for the existence of security considerations (e.g., involvement of the security management function within the SDLC).
- Benchmark the information security organisation (e.g., size, lines of reporting) against similar organisations, and benchmark formalised policies, standards and procedures to international standards/recognised industry best practices.
- Determine if the security management function is commensurate with the size and complexity of the IT landscape. Consider the following:
  – Size, complexity and diversity of the IT landscape
  – Use of security administration tools and technology
  – Alignment of security management to business lines (e.g., do organisation segments have competing security functions?)
  – Skills and training of security management personnel
- Determine if members of executive management communicate the importance and their support of the security management organisation. Consideration should be given to executive management or security steering committee approval of formalised security policies.
- Determine the existence of a management-approved security charter and policies, standards and procedures that address logical security for all relevant aspects of the organisation's IT landscape.
- Determine if the IT security plan has adequately considered the security profile of the organisation, including any regulatory and compliance requirements.
- Assess the ability of the security management organisation to execute and monitor compliance with the plan. Consideration should be given to the size of the organisation, use of security assessment and administration technology and tools, and required experience levels and ongoing training received by security personnel.
- Select policy, standards and procedural documentation from various financial, operational and compliance areas within the organisation, and determine if key provisions of the IT security plan have been appropriately reflected in the documentation.
- Determine if a security review process has been integrated into the organisation's AI and DS processes, requiring security management's involvement and approval of any IT changes that would impact the design or operation systems security.
- Determine if the organisation's AI processes and controls are supported by segregated development, test and assurance, and production environments.
- Identify the existence and reasonableness of anonymous and group accounts (e.g., nobody, web user, everybody), remote processes and started tasks. Consideration should be given to the nature and scope of transaction authorities, the risk of possible escalation of privileges, the process origin (e.g., trusted, non-trusted), or if a security design review was performed for system and application initiated jobs and processes.
- Determine if security software, applications and supporting systems software has been configured to enforce user authentication or propagate user and process identities. Determine if default accounts exist to authenticate anonymous users or processes.
- Determine sources of non-trusted access (e.g., business partners, vendors), and determine how access has been assigned to provide uniquely identifiable account holders and appropriate protection of information.
- Through the use of audit software tools or scripts, identify the existence of inactive or unused accounts and determine the existence of a business justification.
- Identify active vendor or contractor accounts, and determine if access is commensurate with the terms and duration of the contract.
- Determine if vendor-supplied accounts have been appropriately safeguarded (e.g., default passwords changed, accounts revoked).
- Assess the reasonableness of the nature and frequency of verification and vulnerability assessment processes utilised, considering the organisation's risk profile, size, complexity and diversity.
- Determine if security scripts and tools are utilised to test the existence of common vulnerabilities, the effectiveness of security mechanisms and the effectiveness of user access administration processes (e.g., existence of inactive or never used accounts, terminated user accounts, accounts without passwords or forced password changes).
- Identify and select a sample of organisation-critical network devices (hardware and application systems) and at-risk perimeter network devices. Determine the existence of security sensors or use of host logging to capture incidents, and ensure that security incidents are included in the daily review process.

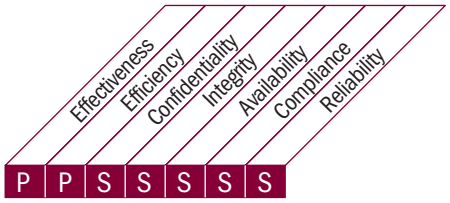
- Obtain a sample of security-related incident work order tickets, and determine if the issue has been appropriately resolved and closed in a timely manner.
- Determine if security tool deployment appropriately addresses all principal technologies utilised by the organisation and if personnel possess the required skills to appropriately operate the security tools and technologies.
- Determine if security personnel are required to attend annual training and if security tools receive routine updates to threat and vulnerability engines and supporting database/signatures.
- Select a sample of business-critical or sensitive data, and determine if data have been secured in accordance with the organisation's encryption standards.
- Verify that the cryptographic system used to protect stored data effectively renders data unreadable, and determine if any method can be utilised to access erased data through forensic techniques.
- Determine whether the security controls have been implemented to prevent exposure from malicious attacks and vulnerabilities.
- Determine if portable code (e.g., Java, JavaScript) and downloaded binaries and executables are scanned before being allowed into the network or blocked from entering the network.
- Determine that the organisation's network documentation accurately reflects the current network environment, including wireless devices, and examine the network design to determine if security barriers are strategically placed at the network's perimeter, between the organisation's trusted internal network and non-trusted public (i.e., Internet), vendor (i.e., service organisation) or business partner (i.e., extranet) segments.
- Verify that changes to security-relevant parameters follow the organisation's change management processes and are authorised and tested accordingly.
- Confirm that sensitive information is not disclosed or exposed to unauthorised parties.

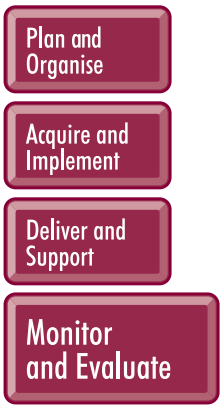
ME2 COBIT COMPONENTS

PROCESS DESCRIPTION

ME2 Monitor and Evaluate Internal Control

Establishing an effective internal control programme for IT requires a well-defined monitoring process. This process includes the monitoring and reporting of control exceptions, results of self-assessments and third-party reviews. A key benefit of internal control monitoring is to provide assurance regarding effective and efficient operations and compliance with applicable laws and regulations.





Control over the IT process of

Monitor and evaluate internal control

that satisfies the business requirement for IT of

protecting the achievement of IT objectives and complying with IT-related laws, regulations and contracts

by focusing on

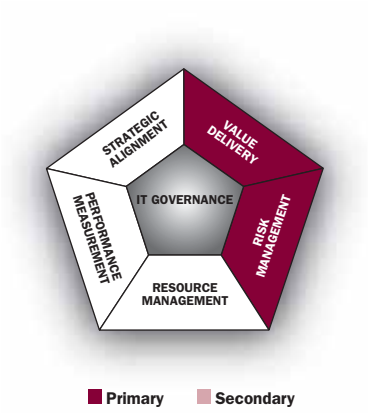
monitoring the internal control processes for IT-related activities and identifying improvement actions

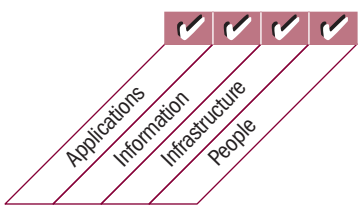
is achieved by

- Defining a system of internal controls embedded in the IT process framework
- Monitoring and reporting on the effectiveness of the internal controls over IT
- Reporting control exceptions to management for action

and is measured by

- Number of major internal control breaches
- Number of control improvement initiatives
- Number and coverage of control self-assessments





ME2 Control Objectives

ME2.1 Monitoring of Internal Control Framework
Continuously monitor, benchmark and improve the IT control environment and control framework to meet organisational objectives.

ME2.2 Supervisory Review
Monitor and evaluate the efficiency and effectiveness of internal IT managerial review controls.

ME2.3 Control Exceptions
Identify control exceptions, and analyse and identify their underlying root causes. Escalate control exceptions and report to stakeholders appropriately. Institute necessary corrective action.

ME2.4 Control Self-assessment
Evaluate the completeness and effectiveness of management's control over IT processes, policies and contracts through a continuing programme of self-assessment.

ME2.5 Assurance of Internal Control
Obtain, as needed, further assurance of the completeness and effectiveness of internal controls through third-party reviews.

ME2.6 Internal Control at Third Parties
Assess the status of external service providers' internal controls. Confirm that external service providers comply with legal and regulatory requirements and contractual obligations.

ME2.7 Remedial Actions
Identify, initiate, track and implement remedial actions arising from control assessments and reporting.

MANAGEMENT GUIDELINES

ME2 Monitor and Evaluate Internal Control

From	Inputs
AI7	Internal control monitoring
ME1	Process performance report

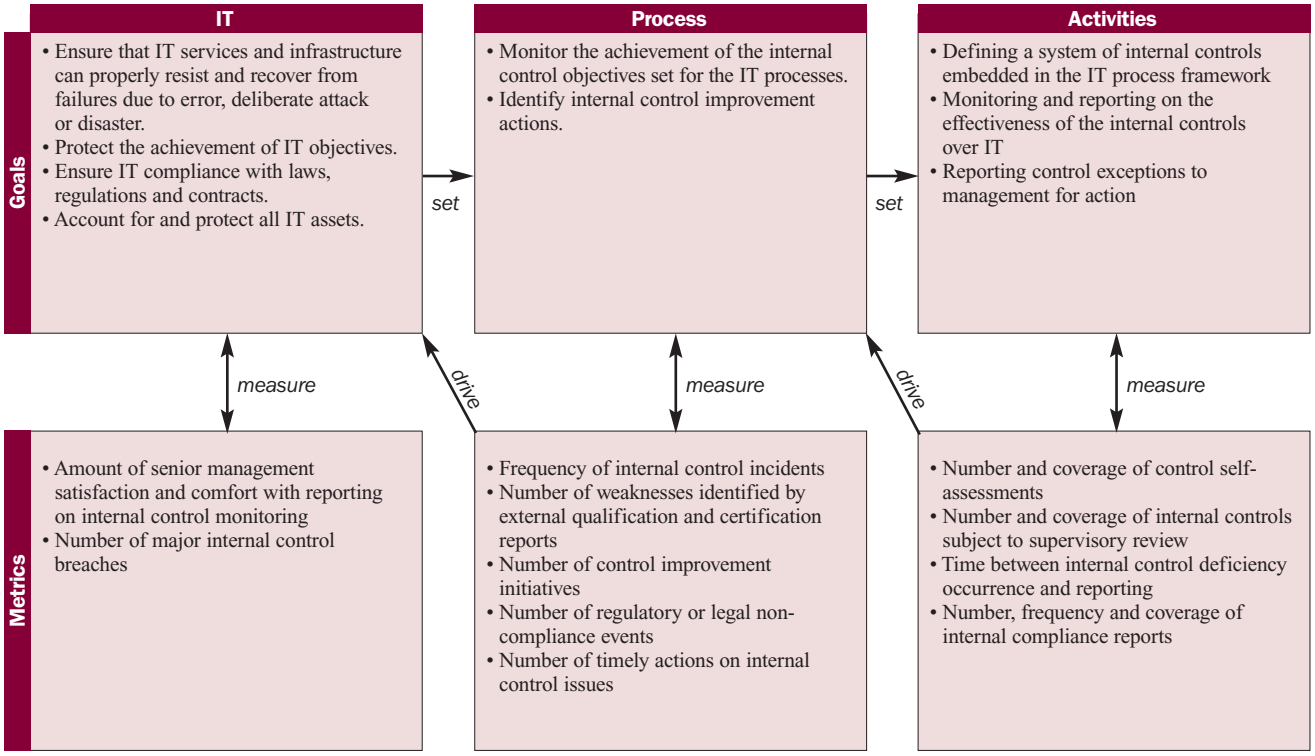
Outputs	To			
Report on effectiveness of IT controls	PO4	PO6	ME1	ME4

RACI Chart

Activities	Board	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Monitor and control IT internal control activities.					A		R		R	R		R
Monitor the self-assessment process.				I	A		R		R	R		C
Monitor the performance of independent reviews, audits and examinations.				I	A		R		R	R		C
Monitor the process to obtain assurance over controls operated by third parties.		I	I	I	A		R		R	R		C
Monitor the process to identify and assess control exceptions.		I	I	I	A	I	R		R	R		C
Monitor the process to identify and remediate control exceptions.		I	I	I	A	I	R		R	R		C
Report to key stakeholders.	I	I	I		A/R							I

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



ME2 Maturity Model

Management of the process of *Monitor and evaluate internal control* that satisfies the business requirement for IT of *protecting the achievement of IT objectives and complying with IT-related laws and regulations* is:

0 **Non-existent** when
the organisation lacks procedures to monitor the effectiveness of internal controls. Management internal control reporting methods are absent. There is a general unawareness of IT operational security and internal control assurance. Management and employees have an overall lack of awareness of internal controls.

1 **Initial/*Ad Hoc*** when
management recognises the need for regular IT management and control assurance. Individual expertise in assessing internal control adequacy is applied on an ad hoc basis. IT management has not formally assigned responsibility for monitoring the effectiveness of internal controls. IT internal control assessments are conducted as part of traditional financial audits, with methodologies and skill sets that do not reflect the needs of the information services function.

2 **Repeatable but Intuitive** when
the organisation uses informal control reports to initiate corrective action initiatives. Internal control assessment is dependent on the skill sets of key individuals. The organisation has an increased awareness of internal control monitoring. Information service management performs monitoring over the effectiveness of what it believes are critical internal controls on a regular basis. Methodologies and tools for monitoring internal controls are starting to be used, but not based on a plan. Risk factors specific to the IT environment are identified based on the skills of individuals.

3 **Defined** when
management supports and institutes internal control monitoring. Policies and procedures are developed for assessing and reporting on internal control monitoring activities. An education and training programme for internal control monitoring is defined. A process is defined for self-assessments and internal control assurance reviews, with roles for responsible business and IT managers. Tools are being utilised but are not necessarily integrated into all processes. IT process risk assessment policies are being used within control frameworks developed specifically for the IT organisation. Process-specific risks and mitigation policies are defined.

4 **Managed and Measurable** when
management implements a framework for IT internal control monitoring. The organisation establishes tolerance levels for the internal control monitoring process. Tools are implemented to standardise assessments and automatically detect control exceptions. A formal IT internal control function is established, with specialised and certified professionals utilising a formal control framework endorsed by senior management. Skilled IT staff members are routinely participating in internal control assessments. A metrics knowledge base for historical information on internal control monitoring is established. Peer reviews for internal control monitoring are established.

5 **Optimised** when
management establishes an organisationwide continuous improvement programme that takes into account lessons learned and industry good practices for internal control monitoring. The organisation uses integrated and updated tools, where appropriate, that allow effective assessment of critical IT controls and rapid detection of IT control monitoring incidents. Knowledge sharing specific to the information services function is formally implemented. Benchmarking against industry standards and good practices is formalised.

ME2 Control Practices

ME2.1 Monitoring of Internal Control Framework
Value drivers:
- IT meeting its objectives for the business
- Reduced impact of control failure or deficiency on the business processes
- Continuous improvement of process controls with respect to industry practices
- Proactive detection and resolution of control deviations
- Compliance with laws and regulations

Risk drivers:
• Increased adverse impact on the organisation's operations or reputation
• Control weaknesses hampering effective business process execution
• Undetected malfunctioning of internal control components

Control practices:
1. Define and implement a policy based on organisational governance standards and industry-accepted frameworks and practices, with associated ongoing internal control monitoring and evaluation activities. Consider organisational governance standards for internal control and risk management.
2. Consider independent evaluations of the IT internal control system (e.g., by internal audit or peers).
3. Identify the boundaries of the IT internal control system (e.g., consider how organisational IT internal controls take into account outsourced development or production activities).
4. Establish processes or procedures to ensure that control activities are in place and exceptions are promptly reported, followed up and analysed. Ensure that appropriate corrective actions are chosen and implemented. Prioritise control exceptions according to the risk management profile (e.g., classify certain exceptions as key risks and others as non-key risks).
5. Maintain the IT internal control system, considering ongoing changes in the organisational control environment, relevant business processes and IT risks. If gaps exist, evaluate and recommend changes.
6. Regularly evaluate the performance of the IT control framework, comparing performance indicators against industry accepted standards and good practices. Consider formal adoption of a continuous improvement approach to internal control monitoring.

ME2.2 Supervisory Review
Value drivers:
• Confirmation that IT processes supporting the achievement of business goals are under effective and efficient control
• Contribution of reviewed results to the overall decision-making process

Risk drivers:
• Control deficiencies hampering the business processes
• Inaccurate or incomplete control deficiency data, resulting in erroneous management decisions

Control practices:
1. Identify and review internal controls that require managerial oversight, considering the criticality and risk of IT process activities. Consider corporate and IT policies on risk management, information security, privacy, and compliance with laws and regulations.
2. Ensure that managerial oversight and review of internal control are appropriately documented.
3. Define an escalation process for issues identified by managerial reviews. Ensure that the process considers the reasons for escalation and the level to which issues are to be escalated. Ensure that the process requires documentation of issues and resulting escalation.
4. Consider implementing automated control monitoring and reporting systems.
5. Ensure that managerial controls are established over the controls included in SLAs with the business and third parties.

ME2.3 Control Exceptions
Value drivers:
• Ability to implement preventive measures for recurring exceptions
• Ability to apply corrective measures in a timely manner
• Enhanced reporting to all affected parties to comply with the defined service levels
• Minimised potential for compliance failures

Risk drivers:
• Control deficiencies not identified in a timely manner
• Management not informed about control deficiencies
• Extended time required to resolve the identified issues, thus decreasing the process performance

Control practices:
1. Establish processes for identifying, reporting, logging and assigning responsibility for reporting and resolving control exceptions (e.g., security breaches, application program abends and network failures). Ensure that the processes address timely reporting and resolution.
2. Considering related business risks, establish policies and standards to establish thresholds for escalation of control exceptions and breakdowns.

3. Communicate procedures for escalation and root cause analysis and reporting same to business process owners and IT stakeholders.
4. Decide which control exceptions should be communicated to the individual responsible for the function and which exceptions should be escalated. Inform affected business process owners and IT stakeholders.
5. Assign accountability for root cause analysis and reporting.

ME2.4 Control Self-assessment
Value drivers:
• Ability to implement preventive measures for recurring exceptions
• Ability to apply corrective measures in a timely manner
• Enhanced reporting to all affected parties to comply with the defined service levels
• Control deficiencies identified before adverse impact occurs
• Proactive approach to improving service quality
• Minimised potential for compliance failures

Risk drivers:
• Control deficiencies not identified in a timely manner
• Management not informed about control deficiencies
• Extended time required to resolve the identified issues, thus decreasing the process performance

Control practices:
1. Define a plan and scope, and identify evaluation criteria for conducting self-assessments. Plan the communication of results of the self-assessment process to IT and general management and the board. Consider internal audit standards in the design of self-assessments.
2. Determine the frequency of periodic self-assessments, taking into account the effectiveness of ongoing monitoring.
3. Assign responsibility for self-assessment to appropriate individuals to ensure objectivity and competence.
4. Provide for independent reviews to ensure objectivity of the self-assessment and enable the sharing of internal control good practices.
5. Compare the results of the self-assessments against industry standards and good practices.
6. Summarise and report outcomes of self-assessments and benchmarking for remedial actions.

ME2.5 Assurance of Internal Control
Value drivers:
• Identification of process control improvement opportunities, resulting in improved service to the business
• Establishment and maintenance of effective internal control framework
• Control skills and knowledge communicated within the organisation to increase the awareness of internal control principles and practice

Risk drivers:
• Processes not effectively controlled and failing to meet the business requirements
• Objective recommendations not obtained, resulting in IT control arrangements not being optimised
• Control gaps not identified
• Compliance with regulatory, contractual and legal requirements not achieved

Control practices:
1. Obtain independent control reviews (e.g., by an internal or external auditor or specialist IT governance consultant), certifications or accreditations. Consider the frequency of reviews in line with the risk profile and business objectives.
2. Ensure that staff members or external specialists are independent and competent to perform reviews, certifications or accreditations (e.g., reviewers hold the Certified Information Systems Auditor™ [CISA®] certification).
3. Confirm that contractual conditions ensure that an adequate scope is performed, liability is established for incorrect opinions and confidentiality is maintained. If a formal certificate is to be obtained, obtain it from an organisation that is an accredited certification authority.
4. Report any significant internal control deficiencies identified for business process owner and IT management attention. Ensure that deficiencies are reported in a manner appropriate for the audience.

ME2.6 Internal Control at Third Parties
Value drivers:
• Identification of service improvement opportunities for third parties
• Confirmation of an effective internal control framework over third-party service providers
• Assurance provided over the service provider's performance and compliance with internal controls

Risk drivers:
- Insufficient assurance over the service provider's control framework and control performance
- Failures of mission-critical systems during operation
- IT services failing to meet the service specifications
- Failures and degradations of service from the provider not identified in a timely manner
- Reputational damage caused by provider service performance degradation

Control practices:
1. Ensure that appropriate internal control requirements are addressed in third-party contract agreements. Where appropriate, ensure that the contract has provisions for audit or review, e.g., certification/accreditation review, an appropriate audit engagement (e.g., SAS 70 Type II engagement), or by direct audit of the service provider by IT management.
2. Ensure that third-party service providers comply with applicable laws, regulations and contractual commitments. Communicate to business process owners, IT management and third-party service providers any failure to comply with such commitments.
3. Confirm receipt of any required legal or regulatory internal control assertions from affected third-party service providers. Investigate exceptions. Obtain assertions from the service provider that appropriate remedial actions will be completed according to an agreed-upon remediation plan.

ME2.7 Remedial Actions
Value drivers:
- Assurance that identified control gaps are remediated as necessary
- Safeguarding of continued functioning of business-critical applications
- Support of the organisation's overall risk management process
- Maintenance of agreed-upon service levels

Risk drivers:
- Previously identified control gaps continuing to cause problems
- Malfunctioning of business-critical applications
- Reputational damage caused by failure to correct service provider control deficiencies

Control practices:
1. Assess control exceptions. Decide which control exceptions must be remediated, in line with the business needs, risk profile and regulatory and compliance requirements. Involve business process owners in the assessment process, where appropriate. Communicate outcomes of the assessment process to the board, senior management, business process owners and IT stakeholders, as appropriate.
2. Design an approach to prioritise and assign responsibility for all control remedial actions.
3. Initiate remedial action tasks based on the agreed-upon approach. Ensure proper tracking and reporting of the status of remedial action tasks.
4. Identify substandard performance in internal control and/or in correcting internal control weaknesses, and specify corrective actions.
5. Escalate continued substandard performance in internal control and/or in correcting internal control weaknesses to business process owners and IT senior management for further action, where appropriate.
6. Approve remedial action tasks upon satisfactory completion against prespecified outcomes.

ME2 IT Assurance Guidelines

Test the Control Design
ME2.1 *Monitoring of internal control framework*
- Assess whether there is executive-level support for organisational governance standards for internal control and risk management (e.g., minutes, corporate policies, interview with CEO). Verify that policies and procedures include governance for internal standards and risk management (e.g., adoption of COSO Internal Control—Integrated Framework, COSO Enterprise Risk Management—Integrated Framework, COBIT).
- Assess whether there is a continuous improvement approach to internal control monitoring (i.e., balanced scorecard, self-assessment).

ME2.2 *Supervisory review*
- Confirm that the internal controls that require supervisory oversight and review are identified and consider the criticality and risk of the related IT process activities (e.g., existence of risk ranking of key processes/controls).
- Confirm that an escalation process for issues identified by supervisory reviews has been defined.
- Understand the automation of control monitoring and reporting.

ME2.3 *Control exceptions*
- Confirm that policies include establishing thresholds for acceptable levels of control exceptions and control breakdowns.
- Confirm that the escalation procedures for control exceptions have been communicated and reported to business and IT stakeholders (e.g., via the intranet, hard-copy procedures). The escalation procedures should include criteria or thresholds for escalations (e.g., control exceptions less than a specific amount of impact do not need to be escalated, control exceptions greater than a specific amount of impact need immediate reporting to CIO, and control exceptions greater than a specific amount of impact require immediate reporting to the board of directors). Interview management to assess knowledge and awareness of the escalation procedures, as well as root cause analysis and reporting.
- Confirm that individuals have been assigned accountability for root cause analysis and reporting as well as exception resolution.

ME2.4 *Control self-assessment*
- Review control self-assessment procedures to ensure the inclusion of relevant information such as scope, self-assessment approach, evaluation criteria, frequency of self-assessment, roles and responsibilities, and results reporting to executive business and IT stakeholders (e.g., reference internal audit standards or accepted practices in the design of self-assessments).
- Corroborate with management to determine if independent reviews of control self-assessment are performed against industry standards and best practices to ensure objectivity and to enable the sharing of internal control good practices (e.g., benchmarking against maturity model levels across similar organisations and the relevant industry).

ME2.5 *Assurance of internal control*
- Verify that independent control reviews, certifications or accreditations are performed periodically according to risk and business objectives along with required external skill sets (e.g., conduct an annual risk assessment and define risk areas for review).
- Verify that the review results have been reported to an appropriate management level (e.g., audit committee) and remedial action has been initiated.

ME2.6 *Internal control at third parties*
- Confirm that internal control requirements are addressed in the policies and procedures for contracts and agreements with third parties, and that appropriate provisions for rights to audit are included.
- Confirm that there is a process in place to ensure that reviews are periodically performed to access the internal controls of all third parties and that non-compliance issues are communicated.
- Confirm that policies and procedures are in place to confirm receipt of any required legal or regulatory internal control assertions from affected third-party service providers.
- Confirm that policies and procedures are in place to investigate exceptions, and obtain assurance that appropriate remedial actions have been implemented.

ME2.7 *Remedial actions*
- Confirm that procedures are established to initiate, prioritise and assign responsibility for all remedial actions, with appropriate tracking of actions.
- Confirm that there is a mechanism to detect substandard performance of the remediation and that corrective actions are identified and reviewed by management (e.g., project milestones). Confirm that continued substandard performance of the remediation is escalated to senior management for further action (e.g., project status reporting, IT steering committee minutes).
- Confirm that established procedures require remedial action tasks to be approved upon satisfactory completion against prespecified outcomes.

Test the Outcome of Control Objectives
- Review internal control monitoring policies and procedures to ensure that they adhere to organisational governance standards, industry-accepted frameworks and industry best practices.
- Determine whether independent assessments of IT controls are required and reports on IT internal control systems are generated for management review.
- Review the independent evaluation reports (e.g., outsourced development or production activities) of the IT internal control system to determine if the proper boundaries are considered and approved by executive management.
- Review and confirm the establishment of processes and procedures to ensure that control exceptions are promptly reported, followed up and analysed.
- Confirm that corrective actions are chosen and implemented to address the control exceptions.
- Review activity logs or pertinent documentation for control exceptions, and confirm that exceptions are promptly reported, followed up, analysed, tracked and corrected.
- Confirm that periodic review is performed to ensure that the IT internal control system is current to recent business changes and the associated business and IT risks.

- Confirm that any gaps between the framework and business processes have been identified and evaluated along with appropriate recommendations. For example, ensure that business systems for operations are not maintained by IT, so established controls policies and procedures used by IT are not applied.
- Confirm that the performance of the IT control framework is regularly reviewed, evaluated, and compared to industry standards and best practices.
- Review the last control exceptions resolution progress status report to confirm that control exceptions monitoring is timely and effective.
- Review control self-assessment schedules, and select a sample of control self-assessment plans and reports to determine if control self-assessments procedures are followed for effective ongoing monitoring.
- Review a sample of the control self-assessment reports for independent review, benchmarking and remedial actions for control exceptions noted (consider ranking the significance of the control exceptions and prioritise remedial actions accordingly).
- Confirm that control self-assessment outcomes and exceptions are reported and there is a process to track control exceptions and remedial actions.
- Assess the competence of external specialists or staff members performing independent reviews for relevant IT audit experience, relevant industry knowledge and appropriate certifications/training.
- Confirm that the personnel performing the reviews are independent (e.g., review the signed confidentiality agreement).
- Review existing contracts for third-party services on IT controls, and validate that the terms and conditions cover clear scope, assignment of liability and confidentiality.
- Confirm that any significant internal control deficiencies identified are reported for immediate management attention.
- Corroborate with members of management to determine if they review the results of third-party compliance review to ensure that third parties comply with required legal, regulatory and contractual obligations.
- Select a sample of the third-party contracts and examine for specification of internal control requirements and establishment of rights to audit provision(s) as appropriate.
- Corroborate to determine if any of the following is performed: certification/accreditation review, appropriate audit engagement (e.g., SAS 70 Type II engagement) or direct audit of the service provider by IT management.
- For a sample of third parties, obtain and review internal control compliance testing reports to ensure that the third-party service providers comply with applicable laws, regulations and contractual commitments.
- Review evidence to ensure that non-compliance issues are communicated and there are remedial action plans (including time frame) in place to address the issues.
- Review the method used to prioritise remediation of control deficiencies for reasonableness.
- Review the list of remediation issues and determine whether those issues are properly prioritised (e.g., critical, high, medium and low).
- Review project scheduling tools and compare to remediation actions to confirm that the areas identified as high risk are adequately prioritised.
- Inspect the sign-offs and determine whether they occurred in a timely manner.

Document the Impact of Control Weaknesses

- Calculate the impact on the organisation for each actual key control failure.
- Quantify the risk and likelihood to the impact on the organisation for each potential key control failure.

COBIT AND RELATED PRODUCTS

The COBIT framework, in versions 4.0 and higher, includes all of the following:
- Framework—Explains how COBIT organises IT governance, management and control objectives and good practices by IT domains and processes, and links them to business requirements
- Process descriptions—Include 34 IT processes covering the IT responsibility areas from beginning to end
- Control objectives—Provide generic best practice management objectives for IT processes
- Management guidelines—Offer tools to help assign responsibility, measure performance, and benchmark and address gaps in capability
- Maturity models—Provide profiles of IT processes describing possible current and future states

In the years since its inception, COBIT's core content has continued to evolve, and the number of COBIT-based derivative works has increased. Following are the publications currently derived from COBIT:
- *Board Briefing on IT Governance, 2nd Edition*—Designed to help executives understand why IT governance is important, what its issues are and what their responsibility is for managing it
- COBIT® Online—Allows users to customise a version of COBIT for their own enterprise, then store and manipulate that version as desired. It offers online, real-time surveys; frequently asked questions; benchmarking; and a discussion facility for sharing experiences and questions.
- *COBIT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition*—Provides guidance on the risks to be avoided and value to be gained from implementing a control objective, and instruction on how to implement the objective. Control practices are strongly recommended for use with the *IT Governance Implementation Guide: Using COBIT® and Val IT™, 2nd Edition*.
- *IT Assurance Guide: Using COBIT®*—Provides guidance on how COBIT can be used to support a variety of assurance activities and offers suggested testing steps for all the COBIT IT processes and control objectives. It replaces the information in the *Audit Guidelines* for auditing and self-assessment against the control objectives in *COBIT 4.1*.
- *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition*—Provides guidance on how to assure compliance for the IT environment based on the COBIT control objectives
- *IT Governance Implementation Guide: Using COBIT® and Val IT™, 2nd Edition*—Provides a generic road map for implementing IT governance using COBIT and Val IT resources and offers a supporting tool kit
- COBIT® *Quickstart*—Provides a baseline of control for the smaller organisation and a possible first step for the larger enterprise
- COBIT® *Security Baseline*—Focuses on essential steps for implementing information security within the enterprise
- COBIT mappings—Currently posted at *www.isaca.org/downloads*:
  - *Aligning COBIT®, ITIL and ISO 17799 for Business Benefit*
  - *COBIT® Mapping: Overview of International IT Guidance, 2nd Edition*
  - *COBIT® Mapping: Mapping of CMMI® for Development V1.2 With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of ISO/IEC 17799:2000 With COBIT®, 2nd Edition*
  - *COBIT® Mapping: Mapping of ISO/IEC 17799:2005 With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of ITIL With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of PMBOK With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of PRINCE2 With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of SEI's CMM for Software With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of TOGAF 8.1 With COBIT® 4.0*

- *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition*—Presents information security in business terms and contains tools and techniques to help uncover security-related problems

Val IT is the umbrella term used to describe the publications and future additional products and activities addressing the Val IT framework.

Current Val IT-related publications are:
- *Enterprise Value: Governance of IT Investments—The Val IT™ Framework*, which explains how an enterprise can extract optimal value from IT-enabled investments and is based on the COBIT framework. It is organised into:
  - Three processes—Value Governance, Portfolio Management and Investment Management
  - IT key management practices—Essential management practices that positively influence the achievement of the desired result or purpose of a particular activity. They support the Val IT processes and play roughly the same role as COBIT's control objectives.
- *Enterprise Value: Governance of IT Investments—The Business Case*, which focuses on one key element of the investment management process
- *Enterprise Value: Governance of IT Investments—The ING Case Study*, which describes how a global financial services company manages a portfolio of IT investments in the context of the Val IT framework

For the most complete and up-to-date information on COBIT, Val IT and related products, case studies, training opportunities, newsletters, and other framework-specific information, visit *www.isaca.org/cobit* and *www.isaca.org/valit*.